Commissaire du
Centre de la sécurité
des télécommunications

RAPPORT ANNUEL 2016-2017

Canada

Bureau du commissaire du
Centre de la sécurité des télécommunications
C.P. 1474, succursale « B »
Ottawa (Ontario) K1P 5P6

Téléphone : 613-992-3044
Télécopieur : 613-992-4096
Site Web : www.ocsec-bccst.gc.ca/

© Sa Majesté la Reine du Chef du Canada, représentée par le
Bureau du commissaire du Centre de la sécurité des télécommunications, 2017

N° de catalogue : D95
ISSN 1206-7490

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

Communications Security
Establis[illegible]t Commissioner

The Honourable Jean-Pierre Plouffe, CD

Juin 2017

Ministre de la Défense nationale
Édifice MGén George R. Pearkes, 13e étage
101, promenade Colonel By, tour Nord
Ottawa (Ontario) K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la ***Loi sur la défense nationale***, j'ai l'honneur de vous transmettre le rapport annuel faisant état de mes activités et constatations pour la période allant du 1er avril 2016 au 31 mars 2017, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Jean-Pierre Plouffe

C.P. / P.O. Box 1474, Succursale « B » / Station "B"
Ottawa ON Canada K1P 5P6

TABLE DES MATIÈRES

Message du commissaire 3

Le mandat et les activités d'examen du commissaire 6

Le point sur les efforts déployés par le CST pour donner suite aux recommandations 9

Aperçu des constatations et des recommandations de 2016–2017 11

Points saillants des rapports présentés au ministre en 2016–2017 13

1. Examen du partage de renseignements du CST avec des entités étrangères 13
2. Examen des activités de collecte du CST menées dans des circonstances exceptionnelles 17
3. Examen des activités du CST relatives aux métadonnées liées à la cyberdéfense 21
4. Étude portant sur la coopération et le partage d'information entre les employés du CST chargés de la sécurité des TI et ceux chargés des renseignements électromagnétiques étrangers afin de contrer les cybermenaces 25
5. Examen annuel des Dossiers relatifs aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures 30
6. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle 34
7. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers et des vérifications ponctuelles des « communications canadiennes » (2015–2016 et 2016–2017) 39

Plaintes concernant les activités du CST 47

Mandat sous le régime de la *Loi sur la protection de l'information* 47

Activités du bureau du commissaire 47

Plan de travail – Examens en cours et prévus 51

Annexe A : Biographie de l'honorable Jean-Pierre Plouffe, CD 53

Annexe B : Extraits de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* relatifs au mandat du commissaire 54

MESSAGE DU COMMISSAIRE

J'ai eu l'honneur en octobre dernier d'être renommé commissaire pour un terme de deux ans. Le renouvellement de ma nomination a coïncidé avec des initiatives gouvernementales visant à étudier les possibilités pour renforcer la reddition de comptes des ministères et organismes fédéraux qui accomplissent des activités liées à la sécurité nationale.

Ces efforts gouvernementaux ont pour but de rassurer les Canadiens que les activités de ces organisations qui visent la protection contre le terrorisme et les cyberattaques – y compris tout autre pouvoir qui pourrait être conféré – ne portent pas atteinte de façon déraisonnable à la vie privée des Canadiens. Mon mandat, ainsi que celui de mes collègues chargés de l'examen au Comité de surveillance des activités de renseignement de sécurité et à la Commission civile d'examen et de traitement des plaintes relatives à la GRC, sont au cœur de ce débat. Le rôle des organismes d'examen existants est d'encourager la transparence et, lorsque l'information doit demeurer secrète, de veiller à ce qu'un examen exhaustif efficace soit effectué pour combler les lacunes en matière d'information dans le débat public. Nous sommes des instruments de reddition de comptes pour nos organisations de sécurité nationale respectives et nous jouons un rôle déterminant afin d'aider à bâtir la confiance du public. À cette fin, je continue de diffuser des statistiques et d'encourager le Centre de la sécurité des télécommunications (CST) à le faire afin d'éclairer la discussion publique et d'améliorer la confiance du public.

Bien que mon rôle à titre de responsable de l'examen indépendant externe soit axé sur le CST, un projet de loi devant le Parlement propose la mise en place d'un comité de parlementaires sur la sécurité nationale et le renseignement qui examinerait les activités relatives à la sécurité dans une optique générale. Je vois d'un œil positif la participation accrue des parlementaires, qui seraient autorisés à recevoir des renseignements secrets, selon le cadre général de reddition de comptes sur les activités liées à la sécurité nationale. Dans ma présentation au comité de la Chambre des communes qui étudiait ce projet de loi, j'ai exposé mes préoccupations selon lesquelles pour éviter le chevauchement, il faut une définition claire des rôles, et j'ai fait valoir que les organismes d'examen devraient, selon la loi, avoir pour mandat de mener des examens conjoints lorsqu'il y a chevauchement, par exemple lorsque le CST travaille avec le Service canadien du renseignement de sécurité. Je suis impatient de travailler avec le comité de parlementaires lorsque celui-ci sera mis sur pied.

Le gouvernement a également tenu des consultations publiques à l'échelle du pays sur la sécurité nationale. Cela m'a permis de présenter mon point de vue sur les sujets déjà abordés, notamment le comité de parlementaires proposé, l'importance de la collaboration entre les organismes d'examen et la façon dont ceux-ci travailleraient avec le comité de parlementaires. Puisque je suis en désaccord, j'ai aussi commenté, en ce qui concerne les autorisations ministérielles pour le CST, les demandes pour l'obtention de mandats judiciaires dans les cas d'interceptions fortuites ou non intentionnelles de communications privées par le CST. En m'appuyant sur mes décennies d'expérience à titre de juge, ainsi que les trois dernières années consacrées à l'examen des activités du CST, j'ai réitéré une proposition en vue du renforcement de la reddition de comptes par le ministre à l'égard du CST. Une meilleure protection de la vie privée pourrait être assurée en ce qui a trait aux autorisations ministérielles si le commissaire du CST évaluait le respect des conditions énoncées dans la ***Loi sur la défense nationale*** avant, plutôt qu'après, la signature des autorisations par le ministre. Ainsi, des « yeux judiciaires » effectueraient une évaluation préalable, impartiale et indépendante de la demande d'autorisation du CST. En effet, le commissaire du CST, qui doit être un juge surnuméraire ou à la retraite d'une cour supérieure et qui doit connaître les questions concernant les autorisations ministérielles et les mesures de protection de la vie privée, procéderait à un examen minutieux.

Lors de ma comparution devant le Comité permanent de la défense nationale de la Chambre des communes en mars, j'ai souligné quatre grandes questions retenant mon attention, dont deux questions abordées ci-dessus. Une troisième question concerne les modifications attendues depuis longtemps à la partie V.1 de la ***Loi sur la défense nationale***. Nous sommes à un moment tournant où la clarté de la législation établissant le mandat du CST, et ce qu'il peut et ne peut pas faire, est essentielle, étant donné qu'il est question de la vie privée des Canadiens. Ainsi, les parlementaires et les membres du public pourraient connaître les autorisations et les restrictions exactes que le CST doit respecter, et être rassurés quant aux mécanismes en place pour veiller à ce qu'il n'y ait pas abus des pouvoirs et, le cas échéant, que ces abus soient mis au jour et traités. La quatrième question stratégique a trait à la nécessité de revoir l'information qui peut être rendue publique dans le but de favoriser la transparence. La transparence a été la pierre angulaire de mon approche en tant que commissaire. Des progrès considérables ont été réalisés à cet égard au Royaume-Uni et aux États-Unis. Il est temps pour le Canada d'en faire autant.

Les progrès réalisés à l'égard de ces questions générales viendront renforcer ma capacité d'accomplir mon mandat premier, soit l'examen des activités du CST, et aideront à créer un cadre de reddition de comptes plus exhaustif et efficace, en assujettissant les ministères et organismes qui mènent des activités relatives à la sécurité nationale, mais qui ne font pas encore l'objet d'un examen, à rendre des comptes.

Pendant que je poursuis ma quatrième année à titre de responsable de l'examen du CST, je suis conscient plus que jamais de l'importance de se tenir au courant des avancées technologiques et opérationnelles au CST et des faits nouveaux externes influant sur celui-ci, dans un monde où les menaces et les technologies, ainsi que le contexte juridique, évoluent constamment. Mon programme d'examen au cours de cette prochaine année continuera de mettre l'accent sur le caractère adéquat des mesures du CST pour protéger la vie privée, le rôle des métadonnées et le partage de renseignements entre le CST et ses partenaires, au pays et à l'étranger. De plus, au cours de la prochaine année, je serai heureux de rencontrer mes homologues des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande pour avoir des discussions et des échanges sur nos expériences respectives dans le domaine de l'examen et de la surveillance, et sur la façon de rendre compte du partage de renseignements entre les organismes de nos pays respectifs, afin d'améliorer la confiance du public.

Lors de l'événement officiel de septembre dernier pour marquer le 20e anniversaire du bureau du commissaire, le ministre de la Défense nationale, qui est responsable du CST devant le Parlement, s'est dit heureux des recommandations et examens indépendants reçus du commissaire du CST et a reconnu l'importance de ce travail à l'appui de sa reddition de comptes à l'égard du CST. Je suis heureux de poursuivre ce rôle essentiel de responsable de l'examen des activités du CST en déterminant si celles-ci sont conformes à la loi, en m'assurant que des mesures de protection robustes sont en place pour protéger la vie privée des Canadiens et en contribuant à la reddition de comptes générale sur les activités relatives à la sécurité nationale.

LE MANDAT ET LES ACTIVITÉS D'EXAMEN DU COMMISSAIRE

Le Bureau du commissaire du Centre de la sécurité des télécommunications (CST) est un organisme d'examen indépendant.

MANDAT

Le mandat du commissaire du CST est énoncé à la partie V.1 de la ***Loi sur la défense nationale*** :

1. procéder à des examens concernant les activités du CST – y compris les activités liées aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information à l'appui du gouvernement du Canada – pour en contrôler la légalité;
2. faire les enquêtes que le commissaire estime nécessaires à la suite d'une plainte écrite; et
3. informer le ministre de la Défense nationale (qui est responsable du CST devant le Parlement) et le procureur général du Canada de toute activité du CST qui, à son avis, pourrait ne pas être conforme à la loi.

En vertu de l'article 15 de la ***Loi sur la protection de l'information***, le commissaire a également pour mandat de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du CST en faisant valoir la primauté de l'intérêt public.

La ***Loi sur la défense nationale*** exige que le commissaire du CST soit un juge surnuméraire ou un juge à la retraite d'une cour supérieure. Elle confère au commissaire une autonomie complète et un accès sans entrave à tous les systèmes et installations du CST, ainsi qu'à son personnel, notamment le pouvoir d'assigner à comparaître pour obliger des particuliers à répondre à des questions. Le commissaire a un budget distinct accordé par le Parlement.

CONSIDÉRATIONS EN MATIÈRE D'EXAMEN

L'approche du commissaire à l'égard des examens est à la fois basée sur les objectifs recherchés – s'appuyant sur son mandat – et préventive. Les activités du CST incluent la collecte de renseignements électromagnétiques étrangers sur des cibles étrangères se trouvant à l'extérieur du Canada, c'est-à-dire de l'information sur les moyens, les intentions ou les activités de cibles étrangères portant sur les affaires internationales, la défense ou la sécurité. Le CST est également l'organisme technique du Canada responsable de la cyberdéfense et de la cryptographie, ainsi que d'autres technologies qui sont requises pour

protéger les systèmes et les réseaux informatiques du gouvernement qui renferment des informations nationales et personnelles sensibles. Le CST a en outre pour mandat de mettre à profit ses capacités uniques afin de fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

Les activités du CST sont distinctes des activités de collecte de renseignements criminels et en matière de sécurité menées par d'autres organismes. Il s'agit dans leur cas d'information sur des activités qui pourraient menacer la sécurité du Canada ou la sécurité publique et que l'on obtient généralement en ciblant des Canadiens en vertu de différents pouvoirs légaux. Il est expressément interdit pour ce qui est des activités du CST de viser des Canadiens ou des personnes se trouvant au Canada. Restreindre la collecte de renseignements à des cibles étrangères à l'extérieur du Canada est compliqué par l'infrastructure de l'information mondiale, qui est interconnectée et en constante évolution, ainsi que par les cibles étrangères, qui sont elles-mêmes astucieuses sur le plan technologique. Le CST a besoin de moyens techniques perfectionnés pour obtenir et analyser l'information et détecter et atténuer les cyberactivités malveillantes. Pour rester efficaces, les méthodes du CST doivent demeurer secrètes.

Dans ce contexte difficile, les agents voués à l'examen doivent posséder des connaissances spécialisées et une expertise pour comprendre les nombreux aspects techniques, juridiques et relatifs à la protection de la vie privée des activités du CST. Ils doivent également posséder des habilitations de sécurité au niveau requis pour examiner les dossiers et les systèmes du CST. Les agents voués à l'examen sont liés par la ***Loi sur la protection de l'information*** et ne peuvent pas divulguer à des personnes non autorisées les renseignements sensibles auxquels ils ont accès.

Une fois une activité sélectionnée pour examen, elle est examinée en fonction de la série de critères standards décrits ci-après :

- **Obligations légales :** le commissaire s'attend à ce que le CST mène ses activités en conformité avec la ***Charte canadienne des droits et libertés***, la ***Loi sur la défense nationale***, la ***Loi sur la protection des renseignements personnels***, le ***Code criminel*** et toute autre législation pertinente.
- **Exigences ministérielles :** le commissaire s'attend à ce que le CST mène ses activités en conformité avec les instructions ministérielles, conformément à toutes les exigences et dans le respect des limites précisées dans une autorisation ou une directive ministérielle.

- **Politiques et procédures :** le commissaire s'attend à ce que le CST dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des instructions suffisantes sur les obligations légales et les exigences ministérielles, notamment en ce qui concerne la protection de la vie privée des Canadiens. Il s'attend à ce que les employés du CST soient au courant des politiques et procédures, et à ce qu'ils s'y conforment. Il s'attend aussi à ce que le CST dispose d'un cadre efficace de validation de la conformité pour assurer le maintien de l'intégrité de ses activités opérationnelles, y compris une reddition de comptes adéquate sur les décisions importantes prises et l'information se rapportant à la conformité et à la protection de la vie privée des Canadiens.

RAPPORTS SUR LES CONSTATATIONS

Rapport classifié au ministre sur chaque examen : Les résultats des examens individuels font l'objet de rapports classifiés au ministre de la Défense nationale. Ces rapports documentent les activités du CST, renferment les constatations relatives aux critères standards et dévoilent la nature et l'importance de tout écart par rapport aux critères. Au besoin, le commissaire formule à l'intention du ministre des recommandations visant à améliorer les mesures de protection de la vie privée ou à corriger les problèmes se rapportant aux activités opérationnelles du CST mis au jour au cours de l'examen. Conformément à la pratique courante de divulgation adoptée par les vérificateurs, le CST reçoit les ébauches des rapports d'examen pour confirmation de l'exactitude des faits. Les constatations et les conclusions sont libres de toute ingérence de la part du CST ou de tout ministre.

Rapport annuel public au Parlement : Le rapport annuel du commissaire est un document public présenté au ministre qui, en vertu de la loi, doit le déposer au Parlement. Le bureau du commissaire publie les titres de tous les rapports d'examen présentés au ministre – 106 à ce jour – sur son site Web.

RESSOURCES DU BUREAU DU COMMISSAIRE

En 2016–2017, le commissaire a été épaulé par 11 employés, eux-mêmes aidés au besoin par des spécialistes en la matière. Les dépenses du bureau se sont élevées à 2 004 378 $, montant qui se situe dans la limite du financement approuvé par le Parlement. Pour en apprendre davantage sur les dépenses du bureau, veuillez consulter son site Web.

LE POINT SUR LES EFFORTS DÉPLOYÉS PAR LE CST POUR DONNER SUITE AUX RECOMMANDATIONS

Le CST a accepté et mis en œuvre, ou travaille à la mise en œuvre, de 95 pour cent (157) des 166 recommandations formulées depuis 1997, y compris les cinq recommandations incluses dans les rapports de cette année. Les commissaires surveillent la façon dont le CST donne suite aux recommandations, aux constatations négatives et aux questions nécessitant un suivi mentionnées dans les examens. Le bureau du commissaire surveille ainsi 16 recommandations actives auxquelles le CST donne suite – 11 recommandations non encore appliquées des années précédentes et cinq de cette année.

Au cours de l'exercice écoulé, le CST a prévenu le bureau qu'il avait donné suite à deux recommandations antérieures.

L'an dernier, dans le cadre de l'examen de l'assistance fournie par le CST au Service canadien du renseignement de sécurité (SCRS) selon la partie *c)* du mandat du CST en ce qui concerne un certain type de rapports mettant en cause des Canadiens (résumé dans le rapport annuel 2015–2016), le commissaire a recommandé que le CST tienne le ministre au courant, sur une base annuelle, de ses activités visées à la partie *c)* de son mandat, soit la transmission au SCRS des rapports mettant en cause des Canadiens qui sont reçus des partenaires de la Collectivité des cinq. Le CST a donné suite à cette recommandation en présentant au ministre un résumé de ces activités.

Le CST a également donné suite à une recommandation découlant de l'examen mené par le bureau des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers (résumé dans le rapport annuel 2014–2015). Cet examen a révélé que le système de minimisation de certains types de métadonnées du CST était décentralisé et dépourvu d'un contrôle et d'une hiérarchisation des priorités adéquats. Le CST ne disposait pas non plus d'un système adéquat de tenue de dossiers. Par conséquent, le commissaire a recommandé que le CST utilise son système actuel de registre centralisé pour consigner les décisions et les mesures prises concernant les nouveaux systèmes de collecte ou ceux qui ont été actualisés, de même que les décisions et les mesures prises concernant la minimisation des métadonnées renfermant de l'information sur l'identité de Canadiens. Le CST a fait savoir qu'il avait mis à jour ses processus de gestion de l'information dans les secteurs responsables des systèmes de collecte dans le but d'améliorer la tenue de dossiers sur les

décisions et les mesures prises, en particulier à l'égard de la minimisation des métadonnées. Le CST continuera de se pencher sur ces processus et de les améliorer, au besoin, en apportant d'autres changements aux politiques et aux processus opérationnels. Le commissaire surveillera aussi ces efforts.

Le commissaire a rappelé au ministre une importante recommandation en suspens résumée dans le rapport annuel 2013–2014 : que le ministre diffuse une nouvelle directive générale à l'intention du CST qui énonce les attentes relatives à la protection de la vie privée des Canadiens lorsque le CST partage des renseignements étrangers. Bien que le partage de renseignements avec ses alliés soit essentiel aux activités de collecte de renseignements électromagnétiques étrangers et à d'autres activités du CST, il pourrait y avoir une incidence directe sur la vie privée et la sécurité des Canadiens lorsqu'une communication privée ou de l'information sur l'identité de Canadiens est partagée. Le ministre a souligné que le CST s'était engagé à donner suite à cette recommandation en priorité.

Le ministre a également souligné l'appel du commissaire au gouvernement à accélérer la mise en œuvre de sa recommandation de 2015 visant à modifier la ***Loi sur la défense nationale*** et la directive ministérielle sur les métadonnées afin de donner un pouvoir exprès et un cadre clair en ce qui concerne la collecte, l'utilisation et la divulgation de métadonnées par le CST.

APERÇU DES CONSTATATIONS ET DES RECOMMANDATIONS DE 2016–2017

Au cours de l'exercice 2016–2017, le commissaire a présenté au ministre neuf rapports classifiés sur ses examens des activités du CST.

Les examens, ainsi qu'une étude, ont été menés sous l'autorité du commissaire :

- pour s'assurer que les activités du CST sont conformes à la loi – comme il est précisé à l'alinéa 273.63(2)*a)* de la ***Loi sur la défense nationale***; et
- pour contrôler la conformité des activités du CST menées sous le régime d'une autorisation ministérielle – comme l'établit le paragraphe 273.65(8) de la ***Loi sur la défense nationale***.

Le premier examen a porté sur le partage de renseignements du CST avec des entités étrangères, autres que ses alliés, en particulier les évaluations du risque visant à déterminer s'il convient ou non d'envoyer ou de demander des renseignements à une entité étrangère lorsque cela pourrait présenter un risque important de mauvais traitements à une personne.

Un examen a porté sur les activités de collecte du CST menées dans des circonstances exceptionnelles, par exemple lorsque le CST est obligé d'acquérir de l'information et de rédiger un rapport concernant des ressortissants de la Collectivité des cinq afin d'appuyer des exigences en matière de renseignements auxquelles il ne serait pas satisfait autrement.

Un autre examen a porté sur les activités du CST relatives aux métadonnées liées à la cyberdéfense. Il s'agissait de la troisième et dernière partie d'une série d'examens exhaustifs visant les activités du CST relatives aux métadonnées.

Le bureau du commissaire a également mené une étude portant sur la coopération et le partage d'information entre les employés du CST chargés de la sécurité des technologies de l'information et ceux chargés des renseignements électromagnétiques étrangers afin de contrer les cybermenaces dans le but d'acquérir des connaissances approfondies de ces activités et de cerner toute question pouvant nécessiter un examen de suivi.

Comme les années précédentes, le commissaire a effectué des examens annuels des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers et à la cyberdéfense, notamment des vérifications ponctuelles des « communications canadiennes » (voir la définition à la page 40) – y compris les communications privées – qui ont été acquises, utilisées, conservées et détruites par le CST, ainsi que des incidents et des erreurs de procédure du

CST liés à la vie privée. L'examen annuel de la divulgation par le CST d'information sur l'identité de Canadiens se poursuivra en 2017–2018.

LES RÉSULTATS

Chaque année, le commissaire présente une déclaration d'ensemble sur ses constatations concernant la légalité des activités du CST. ***Au cours de l'année écoulée, toutes les activités examinées étaient conformes à la loi.***

De même, cette année, le commissaire a formulé cinq recommandations pour promouvoir la conformité à la loi et renforcer la protection de la vie privée, demandant notamment que :

1. les protocoles d'entente avec des entités étrangères précisent clairement les autorisations et les restrictions juridiques du CST, y compris que le CST ne peut pas recevoir, conformément à son mandat de collecte de renseignements électromagnétiques étrangers, de l'information d'entités étrangères qui a été obtenue au moyen d'activités pouvant avoir visé un Canadien ou toute personne au Canada;
2. le CST diffuse des politiques stratégiques générales afin d'établir des mesures de base pour le partage de renseignements avec des entités étrangères;
3. le CST applique uniformément des mises en garde à tous les échanges avec des entités étrangères et utilise des systèmes adéquats afin de consigner tous les renseignements divulgués;
4. en raison des caractéristiques techniques de certaines technologies de communication, les rapports du CST au ministre sur les communications privées renferment des renseignements supplémentaires pour mieux décrire ces communications et expliquer l'ampleur de l'atteinte à la vie privée – la façon dont le CST dénombre actuellement les communications privées donne une vision déformée du nombre de Canadiens ou de personnes au Canada qui sont interlocuteurs dans une communication interceptée par le CST afin d'obtenir des renseignements étrangers sous le régime d'une autorisation ministérielle; et
5. en raison du caractère quasi constitutionnel de la protection accordée aux communications entre un conseiller juridique et son client, le CST obtienne toujours un avis juridique écrit auprès du ministère de la Justice concernant la conservation ou l'utilisation d'une communication interceptée qui est protégée par le secret professionnel de l'avocat.

POINTS SAILLANTS DES RAPPORTS PRÉSENTÉS AU MINISTRE EN 2016–2017

1. Examen du partage de renseignements du CST avec des entités étrangères

CONTEXTE

La capacité du CST à remplir son mandat en matière de sécurité des technologies de l'information et de collecte des renseignements électromagnétiques étrangers repose, dans une large mesure, sur l'établissement et le maintien de relations fructueuses avec ses homologues étrangers. Outre les alliances de longue date que le CST a établies avec ses partenaires de la Collectivité des cinq, les renseignements du CST sont aussi partagés avec d'autres entités étrangères.

La *Loi sur la défense nationale* ne renferme aucun pouvoir explicite ni limite précise concernant le partage de renseignements avec des entités étrangères. De telles activités sont implicitement autorisées par la *Loi sur la défense nationale*.

Le partage de renseignements avec des entités étrangères fait partie intégrante du mandat des organismes canadiens chargés de l'application de la loi et du renseignement, y compris le CST. Pour tenir les ministères et organismes responsables des renseignements partagés à l'extérieur du Canada, le gouvernement du Canada a adopté le *Cadre pour la gestion des risques dans l'échange de renseignements avec des entités étrangères*. Ce cadre établit une approche uniforme à l'échelle du gouvernement exigeant la réalisation d'une évaluation du risque en vue de déterminer si les renseignements doivent être communiqués ou demandés à une entité étrangère lorsque le partage pourrait exposer une personne à un risque important de subir des mauvais traitements. Aux termes d'une directive correspondante du ministre de la Défense nationale, le CST est tenu de gérer le partage de renseignements avec des entités étrangères, appuyé par les politiques orientant les pratiques de partage de renseignements, pour faire en sorte que le partage de renseignements n'engendre pas un risque important de mauvais traitements.

C'était le premier examen réalisé par le bureau à être axé sur le partage de renseignements avec des entités étrangères autres que les partenaires de la Collectivité des cinq. Pour la période allant du 1er février 2010 au 31 mars 2015, le bureau a examiné les éléments suivants :

- le processus de partage de renseignements électromagnétiques étrangers avec des entités étrangères;
- le cadre législatif et stratégique lié au partage de renseignements avec des entités étrangères;
- la question de savoir si le CST avait obtenu auprès d'entités étrangères ou divulgué à des entités étrangères des communications privées ou de l'information sur des Canadiens;
- un échantillon de renseignements échangés, y compris 161 évaluations du risque de mauvais traitements menées aux fins du partage de renseignements; et
- les accords officiels existants avec des entités étrangères.

CONSTATATIONS

Le bureau a conclu que le partage de renseignements du CST avec des entités étrangères pendant la période visée par l'examen était conforme à la loi, au ***Cadre pour la gestion des risques dans l'échange de renseignements avec des entités étrangères*** et aux instructions ministérielles.

Le CST évalue et atténue le risque de mauvais traitements lorsque ses renseignements vont potentiellement être partagés avec des entités étrangères. Le bureau a examiné 161 évaluations du risque de mauvais traitements menées par le CST où le CST a démontré qu'il avait évalué et atténué le risque inhérent au partage de renseignements comme il se doit, et appliqué les critères nécessaires en matière de prise de décisions et d'approbation. Ceci incluait 35 cas où le CST avait partagé des renseignements et que ce partage comportait un risque important de mauvais traitements. Dans ces cas, le CST avait pris des mesures raisonnables pour atténuer le risque, y compris faire respecter les mises en garde et obtenir des garanties auprès des entités étrangères, ou encore, lorsque le risque de mauvais traitements ne pouvait être atténué, le CST avait soupesé correctement le risque de mauvais traitements et celui de ne pas révéler les renseignements, y compris, par exemple, des renseignements liés à une menace pour la sécurité nationale du Canada.

Dans les cas où le CST n'avait pas mené d'évaluation du risque de mauvais traitements avant de partager les renseignements, le bureau n'a vu aucun élément indiquant qu'une évaluation aurait dû être menée.

Le partage de renseignements avec des entités étrangères aide le CST à remplir son mandat, plus particulièrement dans le soutien à la lutte contre le terrorisme et aux opérations militaires, la défense des réseaux informatiques, et la détection des menaces pesant contre les intérêts canadiens de façon générale.

Le CST divulgue rarement de l'information sur l'identité de Canadiens aux entités étrangères. Des 161 évaluations du risque de mauvais traitements examinées, seules 5 avaient donné lieu à la divulgation d'information sur l'identité de Canadiens à une entité étrangère. Dans ces quelques cas, le CST avait mené l'évaluation du risque nécessaire et avait évalué les répercussions sur la vie privée avant d'approuver la divulgation.

Comme le CST traite de l'information découlant de renseignements électromagnétiques, il est peu probable qu'il reçoive de l'information obtenue à la suite de mauvais traitements. Néanmoins, le bureau était convaincu que le CST avait pris des mesures raisonnables pour établir que l'information reçue des entités étrangères n'avait pas été obtenue à la suite de mauvais traitements.

Cela dit, le bureau a relevé des différences dans la manière dont le processus d'évaluation du risque était mis en œuvre par les sections responsables au sein du CST. Les procédures traitant du partage de renseignements sont gérées par deux sections différentes. Si l'une des sections suivait des protocoles uniformes, l'autre tenait des dossiers insuffisants dans certains cas et appliquait les mises en garde relatives au partage des renseignements de façon irrégulière. Toutefois, avant la fin de la période visée par l'examen, cette section avait apporté d'importantes améliorations à la réalisation des évaluations du risque. Le CST a depuis informé le bureau du commissaire qu'il a révisé et normalisé les mises en garde devant être utilisées dans le cadre de toutes les divulgations. Le commissaire s'en assurera dans un examen futur.

Au cours de la période visée par l'examen, le bureau a relevé une absence de politiques stratégiques générales sur le partage de renseignements avec les entités étrangères. Le bureau a également fait état de l'absence de politique stratégique précise sur la réalisation des évaluations du risque de mauvais traitements en vue de partager des renseignements avec des entités étrangères. Le CST a diffusé une nouvelle politique sur ce type d'évaluations du risque après la période visée par l'examen. Néanmoins, au cours de la période visée par l'examen, le CST disposait de politiques et de procédures plus générales d'évaluation du risque établies sur lesquelles se fonder et menait des évaluations régulières de ses ententes sur le partage de renseignements pour veiller à ce que le comportement de ses partenaires demeure compatible avec les intérêts canadiens à l'étranger ou sur le plan de la défense ou de la sécurité.

En menant l'examen, le bureau a soulevé des préoccupations au sujet du fait que les accords officiels existants avec certaines entités étrangères mentionnaient les mesures de protection de la vie privée des Canadiens en des termes généraux seulement. Le bureau s'attendait à ce que les accords conclus par le CST énumèrent de façon explicite les pouvoirs légaux du CST et les restrictions, y compris le fait que dans le cadre de son mandat de collecte de renseignements électromagnétiques, le CST ne peut recevoir aucune communication privée ou toute autre

information obtenue grâce à des activités visant un Canadien. Par la suite, à titre de mesure provisoire, le CST a fourni des lettres aux entités étrangères en question décrivant ses pouvoirs légaux et ses restrictions en attendant que les accords soient modifiés. Le commissaire s'est montré satisfait de cette approche. Il a néanmoins insisté sur la nécessité de conclure ou de modifier à la première occasion tous les accords avec les entités étrangères.

CONCLUSION ET RECOMMANDATIONS

En plus de **recommander** au CST de veiller à ce que les accords officiels conclus avec des entités étrangères précisent ses pouvoirs légaux et ses restrictions, le commissaire **a aussi recommandé** que les mises en garde soient appliquées systématiquement à tous les échanges et que le CST utilise les systèmes adéquats afin de consigner tous les renseignements communiqués. De plus, le commissaire **a recommandé** que le CST publie une politique stratégique générale sur les échanges de renseignements avec des entités étrangères. Le bureau surveillera les efforts déployés par le CST pour donner suite aux recommandations du commissaire et il continuera d'examiner régulièrement les interactions du CST avec les entités étrangères, y compris le partage de renseignements et la réalisation des évaluations du risque de mauvais traitements.

En conséquence de cet examen, le bureau mène un examen distinct sur les pouvoirs du CST en vue de sa participation à une initiative opérationnelle multilatérale axée actuellement sur la menace terroriste qui pèse sur les intérêts occidentaux.

2. Examen des activités de collecte du CST menées dans des circonstances exceptionnelles

CONTEXTE

L'an dernier, le bureau a expliqué les circonstances exceptionnelles dans lesquelles les partenaires du CST de la Collectivité des cinq pouvaient ne pas respecter les accords de coopération conclus entre eux lorsqu'ils obtiennent de l'information ou qu'ils font rapport sur des Canadiens qui se trouvent à l'extérieur du Canada parce que, par exemple, ces Canadiens sont connus pour se livrer à des activités terroristes ou y apporter un soutien. Cette année, l'examen se penchait sur les circonstances exceptionnelles dans lesquelles le CST avait acquis de l'information et rédigé un rapport sur des activités similaires comprenant des ressortissants de la Collectivité des cinq.

PARTENAIRES DE LA COLLECTIVITÉ DES CINQ (*FIVE EYES*)

Les partenaires de la Collectivité des cinq sont le CST et les principaux organismes internationaux des pays de la Collectivité des cinq : la National Security Agency des États-Unis, le Government Communications Headquarters du Royaume-Uni, l'Australian Signals Directorate et le Government Communications Security Bureau de la Nouvelle-Zélande. Ce groupe est également connu sous le terme d'« alliés ».

L'alinéa 273.64(1)*a)* de la *Loi sur la défense nationale* [partie *a)* du mandat du CST] autorise le CST à acquérir et à utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement. Les activités menées dans le cadre de la partie *a)* du mandat du CST :

- doivent correspondre aux priorités du gouvernement du Canada en matière de renseignement;
- ne peuvent viser des Canadiens ou toute personne au Canada; et
- doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés.

Pour pouvoir remplir son mandat de collecte de renseignements électromagnétiques étrangers, le CST s'appuie également sur des relations fructueuses avec ses homologues étrangers.

Les accords de coopération qui existent au sein de la Collectivité des cinq et les résolutions prises par celle-ci comportent un engagement de la part des partenaires à respecter les lois de chacun, les partenaires s'engageant à respecter les droits à la vie privée des ressortissants de chacun. Par conséquent, les politiques et les procédures du CST précisent que les activités de collecte ne doivent pas viser des ressortissants de la Collectivité des cinq, quel que soit le pays où ils se trouvent, ni quiconque se trouvant sur le territoire de la Collectivité des cinq.

Néanmoins, il faut prendre en compte que chacun des partenaires de la Collectivité des cinq est un organisme d'un pays souverain qui peut déroger aux accords s'il y va de l'intérêt national. Dans des circonstances exceptionnelles, le CST peut donc devoir acquérir de l'information comprenant notamment des ressortissants de la Collectivité des cinq ou des étrangers se trouvant sur le territoire de la Collectivité des cinq.

Les relations de longue date qu'entretient le CST avec ses partenaires de la Collectivité des cinq revêtent une importance particulière, puisqu'elles permettent à l'alliance de collaborer dans la poursuite de buts communs tels que l'identification de voyageurs extrémistes qui se rendent, ou qui sont arrivés, dans des zones de conflit pour se joindre à des groupes terroristes ou à d'autres organisations telles Daech et dont le retour éventuel dans leur pays d'origine pourrait représenter une menace.

VOYAGEURS EXTRÉMISTES

On appelle « voyageur extrémiste » (ou « combattant étranger ») une personne soupçonnée de se rendre à l'étranger pour prendre part à des activités liées au terrorisme, par exemple les hommes et les femmes ayant quitté le Canada pour se joindre au groupe terroriste qui se fait appeler « État islamique ».

C'était la première fois que ce type d'activités faisait l'objet d'un examen du bureau du commissaire. Ainsi, l'examen a été l'occasion d'acquérir une connaissance précise de ces activités et des circonstances dans lesquelles elles se déroulent. Les objectifs de l'examen demeuraient bien connus : évaluer si les activités étaient conformes à la loi et à la directive ministérielle liée aux priorités en matière de renseignement et veiller à ce que des mesures adéquates soient prises pour protéger la vie privée des Canadiens dans l'exercice de ces activités.

Pour la période allant de janvier 2015 à août 2016, le bureau a examiné :

- toutes les activités amorcées par le CST qui visaient des ressortissants de la Collectivité des cinq ou des étrangers se trouvant sur le territoire de la Collectivité des cinq;
- les pouvoirs et les politiques, les bases de données et les systèmes connexes du CST;
- les justifications opérationnelles; et
- tout rapport connexe.

CONSTATATIONS

Dans tous les 11 cas, lorsque les activités du CST comprenaient des ressortissants de la Collectivité des cinq partout dans le monde ou quiconque se trouvant sur le territoire de la Collectivité des cinq pendant la période visée par l'examen, le bureau a constaté que les activités étaient conformes à la loi, qu'elles ne visaient pas des Canadiens ou toute personne au Canada et qu'elles correspondaient aux priorités du gouvernement du Canada en matière de renseignement. De plus, les activités de ce type sont rares et représentent un faible risque pour la vie privée des Canadiens.

L'examen a aussi permis de confirmer que les critères énoncés dans la politique du CST étaient respectés : en plus de respecter les exigences prévues par la partie *a)* du mandat du CST, ces activités de collecte particulières ne s'étaient déroulées qu'en des circonstances particulières et limitées, par exemple pour réaliser une priorité du gouvernement du Canada en matière de renseignement qui ne pouvait l'être autrement.

En 2015, le CST a mis à jour sa politique pour pouvoir répondre aux urgences et aux besoins opérationnels plus efficacement et il a officialisé certaines pratiques existantes. Après examen, le bureau a suggéré au CST de préciser sa politique. Le bureau a également constaté que les analystes du CST appliquaient la politique de façon irrégulière, par exemple dans la manière de remplir les formulaires de demande requis et dans la quantité de détails fournis. Le CST a indiqué qu'il travaille à donner suite aux constatations du bureau pour préciser la politique et pour assurer son application appropriée.

CONCLUSION

Vu le nombre limité de ces types d'activités et du faible risque pour la vie privée des Canadiens, le bureau ne les examinera pas régulièrement, mais il surveillera l'ampleur et la nature de ces activités.

Bien que cela ne concerne pas directement l'examen, le commissaire a de nouveau encouragé le ministre à donner suite à la recommandation non encore appliquée de juillet 2013, soit la diffusion d'une nouvelle directive ministérielle pour donner des instructions générales au CST sur ses activités de partage de renseignements électromagnétiques étrangers avec ses partenaires de la Collectivité des cinq. Cet examen avait soulevé la question plus large des relations et des ententes entre les partenaires. Le bureau a été informé qu'une nouvelle directive ministérielle en cours d'élaboration reconnaîtrait explicitement les risques associés à ce type de partage, étant donné que, pour des raisons de souveraineté, le CST ne peut pas exiger que ses partenaires de la Collectivité des cinq rendent compte de toute utilisation de cette information. Le commissaire continuera de surveiller les nouveaux développements.

3. Examen des activités du CST relatives aux métadonnées liées à la cyberdéfense

CONTEXTE

Il s'agit de la troisième et dernière partie d'une série d'examens récents sur les métadonnées, dont les deux premiers – traités dans les deux derniers rapports annuels du commissaire – ont porté sur les activités relatives aux métadonnées liées aux renseignements électromagnétiques étrangers. Cet examen a mis l'accent sur l'utilisation par le CST de métadonnées dans le cadre d'activités de cyberdéfense. L'examen avait pour but de déterminer si les activités du CST relatives aux métadonnées étaient conformes à la loi et ne visaient pas des Canadiens ou toute personne se trouvant au Canada, et que le CST prenait efficacement des mesures satisfaisantes pour protéger la vie privée des Canadiens. Le bureau a examiné les politiques et les procédures opérationnelles du CST, a reçu des séances d'information et des démonstrations techniques et a interviewé le personnel technique et opérationnel du CST.

Le CST mène des activités relatives aux métadonnées liées à la cyberdéfense sous le régime de l'alinéa 273.64(1)*b)* de la ***Loi sur la défense nationale*** et des autorisations ministérielles de cyberdéfense. La directive ministérielle de 2011 sur les métadonnées définit les métadonnées comme « l'information associée à une télécommunication qui est utilisée pour identifier, décrire, gérer ou acheminer la télécommunication ou toute partie de celle-ci, ainsi que son mode de transmission, mais qui exclut toute information ou partie de celle-ci qui pourrait révéler l'objet d'une télécommunication ou l'ensemble ou une partie quelconque de son contenu ». Le CST peut obtenir des métadonnées liées à la cyberdéfense auprès de ses propres sources, de partenaires nationaux et étrangers et de propriétaires de systèmes informatiques importants pour le gouvernement du Canada, y compris les infrastructures essentielles. Le CST utilise les métadonnées pour accomplir cette partie de son mandat afin de détecter et d'atténuer les cybermenaces malveillantes étrangères sophistiquées, et d'aider à protéger les systèmes informatiques importants pour le gouvernement du Canada.

CYBERDÉFENSE

Le CST mène des activités de cyberdéfense. La cyberdéfense aide à protéger les systèmes du gouvernement du Canada contre les États étrangers, les pirates informatiques et les criminels. Le CST suit les menaces partout dans le monde, surveille les réseaux du gouvernement pour détecter les cybermenaces, et travaille avec les ministères à défendre et à renforcer les systèmes qui ont été compromis. Le CST aide à protéger contre le vol l'information ayant une valeur pour le gouvernement, y compris les renseignements personnels.

CONSTATATIONS

Le bureau a confirmé que ses examens antérieurs avaient mis au jour tous les faits concernant les activités du CST relatives aux métadonnées liées à la cyberdéfense. Aucune nouvelle activité ou aucun risque précis de non-conformité ou d'atteinte à la vie privée n'a été recensé. Les métadonnées demeurent essentielles au mandat de cyberdéfense du CST.

Les capacités de détection des cybermenaces du CST permettent de copier et de conserver un sous-ensemble des données du réseau client du gouvernement du Canada – y compris les métadonnées – pour détecter les cyberévénements malveillants étrangers anormaux et sophistiqués et assurer leur analyse continue. De même, le CST ne retient qu'une petite proportion des données passant par ses capteurs de cyberdéfense. Il extrait ensuite les métadonnées des données acquises et s'en sert notamment pour contextualiser la menace et tout maliciel ainsi que pour formuler des conseils pour leur atténuation à l'intention du client et d'autres institutions du gouvernement du Canada.

Les activités de cyberdéfense acquièrent des données se rapportant aux cyberévénements auprès des réseaux du gouvernement du Canada. Il faut s'attendre à ce que les activités de cyberdéfense du CST puissent comprendre des métadonnées concernant des Canadiens puisque les données proviennent de réseaux canadiens situés au Canada – elles sont obtenues par le CST sous le régime d'une autorisation ministérielle ou par les propriétaires de systèmes et les institutions du gouvernement du Canada en vertu du ***Code criminel*** et de la ***Loi sur la gestion des finances publiques*** et sont par la suite divulguées au CST.

Cependant, des examens antérieurs ont montré que les données liées à la cyberdéfense utilisées et conservées par le CST n'impliquent généralement aucun échange de renseignement personnel ou d'autre renseignement important entre l'auteur de la cybermenace étrangère et un fonctionnaire du gouvernement du Canada ou un autre Canadien. Les activités de cyberdéfense du CST permettent généralement d'obtenir des communications ne renfermant qu'un code malveillant ou un élément d'« ingénierie sociale » envoyé à un système informatique pour tromper le destinataire ou compromettre le système.

INGÉNIERIE SOCIALE

L'ingénierie sociale se définit généralement comme un procédé trompeur par lequel des auteurs de cybermenaces conçoivent une situation sociale pour tromper autrui afin d'avoir accès à un réseau autrement fermé, par exemple en faisant en sorte qu'un courriel semble provenir d'une source digne de confiance.

Malgré tout, les mesures de protection de la vie privée que le CST applique à une communication privée s'appliquent également aux métadonnées liées à la cyberdéfense qui pourraient identifier un communicateur ou la communication au Canada – par exemple, les champs « de » et « à » d'un courriel ou une adresse de protocole Internet rattachée à la communication. Le bureau a vérifié si les métadonnées liées à la cyberdéfense concernant un Canadien sont utilisées ou conservées par le CST seulement si elles sont essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada, par exemple lorsqu'elles sont nécessaires pour comprendre les cyberactivités malveillantes étrangères, les capacités ou les intentions, et pour atténuer la menace.

Selon l'information examinée, les séances d'information et les démonstrations techniques reçues et les entrevues menées, le commissaire n'a trouvé aucune donnée probante de non-conformité à la loi. Le CST n'a pas visé, au moyen de ses activités relatives aux métadonnées liées à la cyberdéfense, des Canadiens ou toute personne au Canada.

Les activités du CST relatives aux métadonnées liées à la cyberdéfense sont conformes aux exigences et aux restrictions énoncées dans les directives ministérielles concernant la reddition de comptes et la protection de la vie privée des Canadiens.

Le commissaire était convaincu qu'une série complète de politiques et de procédures opérationnelles du CST concernant la conduite des activités de cyberdéfense offrait une orientation suffisante pour ce qui est des activités relatives aux métadonnées liées à la cyberdéfense. Cela comprend les politiques et les procédures sur : l'utilisation de données de propriétaires de systèmes; la consultation, le traitement et le partage de données; ainsi que la rédaction et la gestion de rapports sur la cyberdéfense. Les entrevues menées auprès des gestionnaires et des employés chargés de la sécurité des technologies de l'information et les observations formulées par eux montrent qu'ils connaissent les politiques et les procédures. Les activités de cyberdéfense du CST font aussi l'objet d'une vérification interne et d'une surveillance continue de la conformité.

CONCLUSION

Le commissaire n'a fait aucune recommandation par suite de cet examen; cependant, il a encouragé le gouvernement du Canada à accélérer la mise en œuvre des recommandations qu'il avait faites en 2015 – et que le commissaire à la protection de la vie privée du Canada avait appuyées – pour modifier la ***Loi sur la défense nationale*** et la directive ministérielle sur les métadonnées afin de donner un pouvoir exprès et un cadre clair en ce qui concerne la collecte, l'utilisation et la divulgation de métadonnées liées aux renseignements électromagnétiques étrangers. Ces modifications devraient comprendre un pouvoir exprès et des mesures de protection de la vie privée pour toutes les activités du CST relatives aux métadonnées, notamment les activités de cyberdéfense visées à la partie ***b)*** du mandat du CST.

Le bureau du commissaire continuera d'examiner les activités du CST relatives aux métadonnées liées à la sécurité des technologies de l'information dans le cadre des examens réguliers des autorisations ministérielles de cyberdéfense, des communications privées utilisées et conservées par le CST, et des divulgations par le CST d'information sur l'identité de Canadiens au gouvernement du Canada et aux partenaires étrangers.

4. Étude portant sur la coopération et le partage d'information entre les employés du CST chargés de la sécurité des TI et ceux chargés des renseignements électromagnétiques étrangers afin de contrer les cybermenaces

CONTEXTE

La complexité de l'infrastructure mondiale d'information augmente de manière exponentielle au fur et à mesure que des personnes, des données et des infrastructures s'y ajoutent. Même si l'expansion offre de nombreux avantages, les systèmes des technologies de l'information (TI) sont également vulnérables pour de nombreuses raisons : ils ne sont généralement pas conçus dans une optique de sécurité, ils sont interreliés, ils servent à stocker une grande quantité de données facilement copiées et ayant une valeur, et la sécurité repose souvent sur une authentification de l'utilisateur qui peut facilement être compromise (p. ex. un mot de passe unique). La distinction entre l'information et la technologie sous-jacente servant à la traiter se brouille; une attaque contre l'une est souvent indissociable d'une attaque contre l'autre.

Les cybermenaces liées à la sécurité des TI se caractérisent par une complexité, une vitesse, une ampleur, une intensité et une portabilité qui augmentent rapidement. La connectivité sans fil et anonyme au réseau mondial est en train de devenir la norme. Les cybermenaces peuvent non seulement toucher les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada, mais elles peuvent aussi être utilisées par des acteurs sophistiqués parrainés par des gouvernements qui constituent une menace pour la sécurité nationale.

Les menaces délibérées comprennent : l'accès ou la divulgation non autorisés, les maliciels, les attaques par déni de service, le piratage d'ordinateurs, la mystification, l'hameçonnage, l'altération et les menaces internes. Il existe en outre les menaces liées aux accidents et aux dangers naturels.

Dans ce contexte changeant, les employés du CST chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI ont collaboré de plus en plus étroitement à l'échange de données et à l'analyse des cybermenaces et des atteintes touchant les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. En 2009, le CST a créé le Centre d'évaluation des cybermenaces (CECM) pour assurer une plus grande coordination et synchronisation entre les employés du CST chargés de la sécurité

des TI et ceux chargés des renseignements électromagnétiques étrangers. Le CECM agit également à titre de point d'accès du gouvernement du Canada au CST pour toutes les questions de cyberdéfense.

En octobre 2010, la Stratégie de cybersécurité du Canada a été diffusée et le CST a reçu des fonds qui ont permis aux employés du CST chargés de la sécurité des TI et à ceux chargés des renseignements électromagnétiques étrangers de partager plus facilement de l'information concernant les cybermenaces.

Les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI sont guidés par leur partie respective du mandat législatif du CST. Les activités des employés du CST chargés des renseignements électromagnétiques étrangers sont régies par l'alinéa 273.64(1)*a)* de la ***Loi sur la défense nationale*** (partie *a)* du mandat du CST) : acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers. Les activités des employés du CST chargés de la sécurité des TI sont régies par l'alinéa 273.64(1)*b)* de la ***Loi sur la défense nationale*** (partie *b)* du mandat du CST) : fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. L'une des fonctions premières des employés chargés de la sécurité des TI est de placer des capteurs sur les passerelles de réseau du gouvernement du Canada pour la détection des cybermenaces. Les données recueillies peuvent ensuite être transmises aux employés chargés des renseignements électromagnétiques étrangers, qui s'en servent pour orienter la collecte de renseignements étrangers sur des acteurs hostiles.

En vertu de la ***Loi sur la défense nationale***, les employés chargés de la sécurité des TI et ceux chargés des renseignements électromagnétiques étrangers ne peuvent pas mener d'activités visant des Canadiens ou toute personne au Canada et doivent prendre des mesures pour protéger la vie privée des Canadiens. Cependant, les renseignements échangés et consultés sur les cybermenaces peuvent inclure des communications privées et de l'information sur l'identité de Canadiens; c'est d'ailleurs l'une des raisons pour lesquelles le bureau du commissaire a entrepris cette étude. Celle-ci a été menée sous l'autorité du commissaire, tel qu'il est énoncé à l'alinéa 273.63(2)*a)* de la ***Loi sur la défense nationale***.

Les objectifs de l'étude étaient les suivants : acquérir des connaissances détaillées et documenter la coopération et le partage d'information sur les activités liées aux cybermenaces entre les employés du CST chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI; observer la connaissance qu'ont les employés du CST des autorisations pertinentes; déterminer les activités, le cas échéant, qui pourraient soulever des questions concernant le risque de conformité à la loi ou la protection de la vie privée des Canadiens; et, s'il y a lieu, cerner toute question qui pourrait nécessiter un examen de suivi.

OBSERVATIONS

Lorsqu'ils analysent les activités liées aux cybermenaces, les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI partagent outils et locaux; c'est pourquoi les deux équipes ont accès à des données obtenues selon les parties *a)* et *b)* du mandat du CST. Cela est voulu : ainsi, les deux équipes peuvent effectuer des analyses exhaustives des cybermenaces. Les restrictions d'accès aux données visées aux parties *a)* et *b)* sont fonction des paramètres détaillés dans les politiques et les procédures de l'équipe chargée des renseignements électromagnétiques étrangers et de celle chargée de la sécurité des TI. Les analystes des deux équipes doivent respecter toutes les politiques et les procédures connexes lorsqu'ils traitent des données de l'autre équipe. Les analystes de l'équipe chargée des renseignements électromagnétiques étrangers qui prêtent main-forte à l'équipe chargée de la sécurité des TI concernant les cybermenaces reçoivent l'autorisation de mener des activités de cyberdéfense selon la partie *b)* du mandat du CST.

Chacun de ces employés du CST reçoit une formation et doit passer les tests sur les politiques applicables à ses responsabilités et à celles de ses pairs selon le mandat. En raison de la complexité des politiques et des procédures, des personnes désignées supervisent et dirigent la mise en œuvre opérationnelle de ces lignes directrices.

Même si chaque employé reçoit une formation pour accomplir les tâches attribuées selon, soit la partie *a)*, soit la partie *b)* du mandat du CST, la mise en application des politiques, la séparation des données liées à la sécurité des TI et aux renseignements électromagnétiques étrangers, ainsi que l'utilisation d'outils analytiques distincts, sont du ressort des superviseurs. En attribuant des tâches selon, soit la partie *a)*, soit la partie *b)* du mandat du CST, le superviseur est en mesure de surveiller la conformité.

D'après le CST, les données que les employés chargés de la sécurité des TI partagent avec ceux chargés des renseignements électromagnétiques étrangers ne peuvent être utilisées qu'aux fins auxquelles elles ont été recueillies, c'est-à-dire la cyberdéfense. En règle générale, les analystes de l'équipe chargée des renseignements électromagnétiques étrangers et ceux de l'équipe chargée de la sécurité des TI travaillent en autonomie puisque les obligations légales et les exigences des politiques en ce qui concerne l'utilisation, la conservation et la divulgation de renseignements diffèrent en fonction du mandat applicable. Ainsi, la divulgation de renseignements personnels entre les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI n'est possible qu'après que des obligations légales précises ont été remplies.

Les deux équipes opérationnelles du CST peuvent communiquer des renseignements personnels aux termes des alinéas 8(2)*a)* et *b)* de la ***Loi sur la protection des renseignements personnels***. Selon l'alinéa 8(2)*a)*, la communication de

renseignements personnels est autorisée puisqu'elle se fait aux fins auxquelles ceux-ci ont été recueillis ou préparés par l'institution, ou pour les usages qui sont compatibles avec ces fins (détection des activités liées aux cybermenaces étrangères, que ce soit aux fins de collecte de renseignements étrangers ou de cyberdéfense). Selon l'alinéa 8(2)*b*), la communication est aussi autorisée puisqu'elle se fait aux fins qui sont conformes avec les lois fédérales (alinéa 273.64(1)*a*) ou *b*) de la *Loi sur la défense nationale*).

Le commissaire est d'avis que les activités de coopération et de partage d'information entre les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI afin de contrer les cybermenaces sont conformes aux pouvoirs prévus par la *Loi sur la défense nationale* et la *Loi sur la protection des renseignements personnels* et que l'information actuellement partagée entre ces employés présente un risque minimal pour la vie privée des Canadiens.

Les renseignements sur les cybermenaces recueillis et diffusés au sein du CST présentent un risque moindre pour la vie privée que d'autres types de renseignements recueillis selon la partie *a*) du mandat du CST. Le bureau du commissaire a plusieurs fois remis en question la pratique du CST, dans le cadre de ses opérations de cyberdéfense en vertu d'une autorisation ministérielle, qui consiste à traiter tous les courriels à destination ou en provenance du Canada interceptés de façon non intentionnelle comme des communications privées selon la définition du *Code criminel*. Tel qu'il a aussi été mentionné dans le cadre de l'examen des autorisations ministérielles de cyberdéfense de cette année, le commissaire est d'avis qu'une communication qui ne contient rien de plus qu'un code malveillant et/ou un élément d'ingénierie sociale, envoyé par un auteur de cybermenace se trouvant à l'extérieur du Canada, dont on peut raisonnablement penser qu'elle a pour but de compromettre les systèmes ou les réseaux informatiques du gouvernement du Canada, ne constitue pas une communication privée au sens du *Code criminel*.

Par ailleurs, en ce qui concerne les activités de cyberdéfense, la préoccupation n'est pas le contenu de la communication, mais bien l'information qui aide à attribuer la cybermenace à son auteur et au vecteur de menace. Il est rare que le contenu d'une communication donnée fournisse des renseignements permettant de déterminer l'origine d'un vecteur de menace ou les mesures d'atténuation qui devraient être prises. Cependant, ces renseignements sur la cybermenace pourraient renfermer de l'information sur l'identité de Canadiens qui est essentielle au mandat de cyberdéfense du CST.

Pour les cas où de l'information sur l'identité de Canadiens serait obtenue dans le cadre de ces activités, le CST a adopté des mesures afin de protéger la vie privée des Canadiens – sous forme de politiques et de procédures et d'éléments intégrés aux technologies. L'étude a révélé que l'équipe chargée des renseignements

électromagnétiques étrangers et celle chargée de la sécurité des TI disposent de politiques et de procédures exhaustives relativement à ces activités, et qu'une surveillance de la conformité est assurée.

Pendant la tenue de cette étude, le bureau a demandé au CST de lui fournir un avis juridique pertinent. Contrairement à la pratique établie depuis longtemps, le CST n'a pas fourni d'avis et a plutôt présenté un résumé. Par le passé, le CST a toujours donné accès à ses avis juridiques au bureau du commissaire, étant entendu qu'il n'était pas renoncé au privilège du secret professionnel de l'avocat. Cependant, le commissaire est reconnaissant du fait que le CST a depuis présenté au bureau des avis juridiques pertinents pour d'autres examens en cours. Lorsqu'on procède à des examens d'activités pour en contrôler la légalité, il est essentiel de savoir comment la loi est interprétée, et si, et comment, elle est appliquée par l'organisme.

CONCLUSION

L'étude a donné au bureau du commissaire l'occasion de se renseigner sur les subtilités de l'échange d'information entre les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI, et de déterminer si des secteurs ou des activités doivent faire l'objet d'un examen de suivi.

Le commissaire n'avait pas d'autres questions concernant la conformité à la loi ou la protection de la vie privée des Canadiens. L'étude n'a pas mis au jour de nouvelles questions nécessitant un examen de suivi. Toutefois, l'utilisation par le CST d'une base de données et d'un outil utilisés pour la détection de cybermenaces fait l'objet d'un examen approfondi dans le cadre d'un examen continu.

Le bureau continuera d'examiner les activités de coopération et de partage d'information entre les employés chargés des renseignements électromagnétiques étrangers et ceux chargés de la sécurité des TI afin de contrer les cybermenaces dans le cadre des examens des activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense menées sous le régime d'une autorisation ministérielle, ainsi que des divulgations d'information sur l'identité de Canadiens.

5. Examen annuel des Dossiers relatifs aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures

CONTEXTE

Le CST signale et documente tout incident associé à ses activités opérationnelles ou à celles de ses alliés où il pourrait y avoir eu atteinte à la vie privée d'un Canadien, contrairement aux politiques ou aux procédures opérationnelles du CST en matière de protection de la vie privée des Canadiens.

Ces incidents, ainsi que les mesures correctives prises, sont consignés dans un de trois dossiers en fonction de l'endroit où l'incident est survenu et de son potentiel de causer un dommage. Il s'agit du Dossier relatif aux incidents liés à la vie privée (DIVP), du Dossier relatif aux incidents liés aux alliés (DIA), récemment créé, et du Dossier des erreurs de procédure mineures (DEPM) tenus par le CST.

Le DIVP est un dossier des incidents attribuables au CST concernant de l'information sur un Canadien ou toute personne au Canada qui a été traitée de manière contraire à la politique de protection de la vie privée du CST et qui a été exposée à des parties externes ne devant pas les avoir reçues. Ce type de manipulation inadéquate est désigné « incident lié à la vie privée ». Le DIA est un dossier des incidents liés à la vie privée qui sont attribuables à des alliés. Ces incidents peuvent être signalés par les partenaires mêmes ou par le CST. Enfin, le DEPM est un dossier des cas où le CST a traité de manière inappropriée de l'information sur un Canadien, mais où l'information a été contenue au sein du CST et n'a pas été exposée à des parties externes.

L'examen annuel par le bureau du DIVP, du DIA et du DEPM met l'accent sur les incidents qui n'ont pas été examinés en détail dans le cadre d'autres examens. L'examen offre une occasion de déterminer les tendances ou les faiblesses systémiques qui pourraient indiquer que des mesures correctives, des changements aux procédures ou aux politiques du CST ou un examen approfondi d'une activité ou d'un incident précis s'imposent. Par exemple, le bureau pourrait exercer une fonction d'examen critique afin de déterminer si l'un des incidents survenus dans le cadre des opérations constituait une « atteinte substantielle à la vie privée », ce que la politique pangouvernementale définit comme une atteinte visant des renseignements personnels sensibles dont on peut raisonnablement penser qu'elle risque de causer un préjudice ou un dommage sérieux à la personne, ou touche un nombre élevé de personnes.

En plus d'examiner les erreurs de procédure, les incidents et les mesures subséquentes prises par le CST pour corriger la situation ou atténuer les répercussions, l'examen avait les objectifs suivants : se pencher sur toute atteinte substantielle à la vie privée dans le cadre des opérations, ainsi que les mesures correctives connexes du CST; déterminer si tout incident soulève des questions de conformité à la loi ou de protection de la vie privée des Canadiens; et évaluer le cadre de validation de la conformité à la politique du CST et les activités de surveillance dans ce contexte.

Bien que ces examens couvrent normalement une année civile entière, cet examen a porté sur six mois : du 1er janvier 2016 au 30 juin 2016. Les examens futurs de ces dossiers couvriront une période de 12 mois, soit du 1er juillet au 30 juin, plutôt que l'année civile. On a modifié la période pour tenir compte de la charge de travail du bureau relative à la production de rapports à la fin de l'exercice.

Le bureau a examiné 55 incidents liés à la vie privée consignés dans le DIVP et le DIA, ainsi que les mesures correctives prises par le CST pour y remédier. Le bureau a également examiné les 6 erreurs de procédure mineures documentées par le CST au cours de la période visée.

CONSTATATIONS

Les incidents liés à la vie privée incluaient, par exemple, le partage d'information sur l'identité de Canadiens ou son intégration par inadvertance à un rapport sans la supprimer, comme l'exige la politique du CST, ainsi que le ciblage non intentionnel ou les recherches dans les bases de données visant des renseignements sur des personnes jusqu'alors non connues pour être des Canadiens ou des personnes au Canada. Dans tous les cas, les rapports ont été annulés ou corrigés et l'information sur l'identité a été dûment supprimée, ou le CST a radié toute communication interceptée ou tout rapport connexe.

INFORMATION SUR L'IDENTITÉ DE CANADIENS

L'information sur l'identité de Canadiens est celle pouvant être utilisée pour identifier un Canadien ou une organisation ou une société canadienne dans le contexte de renseignements personnels ou commerciaux. L'information sur l'identité de Canadiens comprend, sans s'y limiter, les noms, les numéros de téléphone, les adresses de courriel, les adresses de protocole Internet et les numéros de passeport. Lorsque le CST intègre de l'information sur l'identité de Canadiens à un rapport, il doit la supprimer et la remplacer par une mention générique, telle que « Canadien nommé », afin de protéger l'identité de ce Canadien.

L'examen a mis au jour deux cas où des rapports renfermant de l'information non supprimée sur l'identité de Canadiens ont été annulés, mais n'ont pas été radiés des bases de données du CST. Le CST a donc manuellement retiré ces rapports du système. Deux incidents concernaient le partage au sein du CST de rapports d'un allié renfermant de l'information sur un Canadien ou une personne au Canada qui ont été transmis au Service canadien du renseignement de sécurité par le CST et qui auraient dû faire l'objet d'une diffusion interne restreinte. (L'examen mené par le bureau au sujet du soutien apporté par le CST au Service canadien du renseignement de sécurité concernant ce type de rapports a été souligné dans le rapport annuel du dernier exercice.) À la suite de ces deux incidents, le CST a notamment donné une formation de rattrapage aux employés en cause, ainsi qu'à ceux susceptibles de traiter ces types de rapports.

Pour ce qui est des erreurs de procédure mineures, le commissaire a convenu avec le CST qu'il s'agissait d'erreurs mineures ne constituant pas des « incidents liés à la vie privée ». Ces erreurs de procédure incluaient, par exemple : un dossier renfermant des données non visionnées et peut-être des communications privées qui ont été conservées au-delà du délai prescrit; de l'information sur l'identité de Canadiens qui a accidentellement été mise à la disposition de destinataires non concernés au sein du CST; et des non-Canadiens qui ont brièvement eu accès à, mais n'ont pas consulté, des données limitées sur la cyberdéfense. Ces incidents sont considérés avoir un effet moindre sur la vie privée puisqu'ils restent à l'interne et qu'ils sont réglés avant que quelqu'un à l'extérieur du CST ne consulte l'information.

Après examen des trois dossiers, des réponses obtenues du CST, ainsi que des dossiers connexes du CST, le commissaire a conclu que, dans tous les cas, le CST a pris les mesures correctives appropriées, y compris, le cas échéant, des mesures pour prévenir des occurrences similaires à l'avenir.

Selon la politique pangouvernementale, il incombe au ministère ou à l'organisme de signaler les atteintes substantielles à la vie privée. Le CST n'a pas signalé d'atteinte substantielle à la vie privée dans le cadre de ses opérations pour la période visée. Le commissaire a convenu que les incidents énumérés dans le DIVP et le DIA pour la période visée ne constituaient pas des atteintes substantielles à la vie privée.

Cet examen a tiré parti des renseignements supplémentaires que le CST a fournis pour décrire et documenter en profondeur chaque incident afin de donner suite à la recommandation du commissaire découlant de l'examen de ces dossiers du dernier exercice. Les inscriptions aux dossiers étaient beaucoup plus détaillées et incluaient une description et un échéancier des incidents, les raisons de l'occurrence, les mesures correctives, ainsi que toute activité de suivi prévue. La séparation des incidents concernant le CST et de ceux concernant les alliés a permis une plus grande clarté. Une autre nouveauté qui a renforcé les mesures

de protection de la vie privée des Canadiens a été le nouvel instrument de politique, lequel énonce les procédures à suivre par les employés du CST pour traiter les incidents liés à la vie privée et les erreurs de procédure.

CONCLUSION

Cet examen n'a pas mis au jour des atteintes substantielles à la vie privée, des lacunes systémiques ou des questions nécessitant un examen de suivi qui n'était pas déjà prévu. Le CST a affirmé ne pas avoir eu connaissance d'une quelconque incidence négative sur les Canadiens concernés par un des incidents liés à la vie privée.

Le commissaire était convaincu que le CST a réagi comme il se doit aux incidents liés à la vie privée et aux erreurs de procédure mineures relevés durant la période visée.

L'enregistrement et le signalement des incidents liés à la vie privée et des erreurs de procédure mineures demeurent un moyen efficace pour le CST de promouvoir le respect des obligations légales, des exigences ministérielles et des politiques et procédures opérationnelles, et d'améliorer la protection de la vie privée des Canadiens. Les améliorations apportées aux rapports et aux structures de dossiers connexes devraient permettre de renforcer les mesures de protection de la vie privée.

Le commissaire n'a formulé aucune recommandation. Toutefois, il a encouragé le CST à chercher un moyen pratique de s'assurer que les rapports annulés renfermant de l'information sur l'identité de Canadiens sont rapidement retirés de ses bases de données, et qu'il y a confirmation de l'annulation. De plus, il s'agit du deuxième examen consécutif du DIVP qui a mis au jour une diffusion inappropriée d'information sur l'identité de Canadiens en ce qui concerne des rapports d'alliés contenant de l'information sur un Canadien ou une personne au Canada. Le commissaire s'est engagé à intégrer ces incidents au prochain examen de suivi du soutien apporté par le CST au Service canadien du renseignement de sécurité en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens.

6. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle

CONTEXTE

La *Loi sur la défense nationale* confère au CST le mandat de mener des activités de sécurité des technologies de l'information, notamment fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. Ces activités, connues comme la partie ***b)*** du mandat du CST, ne doivent pas viser des Canadiens, où qu'ils se trouvent, ou toute personne au Canada et elles doivent faire l'objet de mesures pour protéger la vie privée des Canadiens en ce qui a trait à l'utilisation et à la conservation des renseignements interceptés [alinéas 273.64(2)***a)*** et ***b)*** de la *Loi sur la défense nationale*].

Aux termes du paragraphe 273.65(3) de la *Loi sur la défense nationale*, le ministre peut – dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada contre les cybermenaces – autoriser par écrit le CST à intercepter des communications privées qui sont liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Pour détecter et contrer les cybermenaces sophistiquées, le CST peut, à la réception d'une demande écrite d'une institution du gouvernement du Canada en vue de la conduite d'activités de sécurité des technologies de l'information, prendre des mesures pour recueillir et analyser des données du système ou du réseau de ce client. Ces activités sont connues comme étant des activités de cyberdéfense. Étant donné que ces activités pourraient entraîner l'interception de communications privées, le CST doit mener ces activités sous le régime d'une autorisation ministérielle. Une autorisation ministérielle est valide pendant un an.

L'objectif premier de cet examen était d'évaluer la conformité à la loi des activités de cyberdéfense du CST, ainsi que la mesure dans laquelle le CST protège la vie privée des Canadiens en menant ces activités. On a prêté une attention particulière à l'interception et à l'utilisation par le CST de communications privées et d'information sur des Canadiens.

L'examen, qui a porté sur l'autorisation ministérielle de cyberdéfense en vigueur du 1er juillet 2015 au 30 juin 2016, a permis de donner suite aux constations et aux recommandations du rapport de l'an dernier.

CONSTATATIONS

Le commissaire a conclu que l'autorisation ministérielle de cyberdéfense de 2015-2016 respectait les conditions d'autorisation énoncées dans la ***Loi sur la défense nationale***.

Le commissaire n'a trouvé aucune donnée probante selon laquelle le CST aurait mené toute activité visée par l'autorisation ministérielle de cyberdéfense qui serait contraire à la loi. Dans l'ensemble, le CST n'a apporté aucun changement important à la façon dont les activités de cyberdéfense sont menées, ou des changements qui auraient présenté un risque pour la conformité à la loi ou la protection de la vie privée.

Les changements apportés à l'autorisation ministérielle en soi relative à la cyberdéfense de 2015-2016 n'étaient pas importants; ils étaient toutefois positifs. Les éclaircissements apportés par les changements aux mémoires de demande connexes adressés au ministre étaient également positifs.

Depuis l'examen réalisé l'an dernier, le CST a apporté un changement de taille à sa politique sur la cyberdéfense qui a élargi le nombre de situations où certaines informations sur l'identité de Canadiens associées à une infrastructure ciblée ou à laquelle il a été porté atteinte peuvent être divulguées, sans suppression, à des institutions du gouvernement du Canada, à des entités du secteur privé et à des alliés choisis lorsque cette information est nécessaire aux fins d'analyse et d'atténuation des vulnérabilités cybernétiques. Le commissaire a accepté le changement en raison des attentes relatives à la vie privée plus faibles rattachées à ce type d'information sur l'identité de Canadiens. D'après le CST, le changement l'aidera à jouer son rôle d'atténuation des cybermenaces dans le cadre de la Stratégie de cybersécurité du Canada, par exemple, en facilitant la communication en temps opportun des renseignements sur les cybermenaces aux propriétaires des données et aux partenaires. Toutefois, le CST devrait travailler avec ses alliés à mettre au point une entente sur le partage de renseignements aux fins de la cybersécurité, qui n'était qu'une ébauche au moment de rédiger le rapport.

Le bureau du commissionnaire continue de suivre la mise en œuvre d'un service introduit en 2014-2015 qui est utilisé pour détecter et atténuer la cyberactivité malveillante ou anormale visant les appareils de communication électronique. Le bureau surveillera également l'utilisation par le CST d'un outil qui avait été déployé dans le cadre d'un projet pilote pendant la période visée par l'examen. Ces nouveaux services semblent généralement bien convenir aux activités liées à la cyberdéfense actuelles du CST, et ce dernier applique aux nouveaux services les politiques et procédures opérationnelles en place, le cadre de validation de la conformité ainsi que des mesures de protection de la vie privée.

Au cours de la période visée par l'examen, le CST a modernisé la base de données qui contient les données pour la cyberdéfense utilisées et conservées ainsi que le système de consignation des communications privées connexes. Les données que contient cette nouvelle base de données sont utilisées, pour la plupart, pour l'analyse des cybermenaces et la rédaction de rapports. La base de données offre des capacités accrues de tenue de dossiers, et des renseignements plus détaillés doivent y être consignés sur les motifs de la conservation d'une communication privée, ce qui permet au CST de mieux démontrer la conformité. La base de données se sert également des attributs des données interceptées pour automatiser l'identification d'éventuelles communications privées. Ceci devrait réduire le nombre d'erreurs humaines et normaliser le dénombrement des communications privées de cyberdéfense. Cette automatisation donne également suite à la recommandation formulée par le commissaire l'an dernier de renforcer l'exactitude et la cohérence dans les rapports au ministre. Le bureau du commissaire continuera de surveiller le suivi fait par le CST des communications privées de cyberdéfense et les rapports à cet égard.

Les données interceptées, y compris les communications privées, peuvent être conservées ou utilisées par le CST seulement si l'interception était nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada. Un incident cybernétique peut comporter un ou plusieurs cyberévénements et une ou plusieurs communications privées. Le bureau du commissaire a sélectionné et examiné un échantillon de données de cyberdéfense que le CST a interceptées en 2015–2016, y compris la majorité (environ 75 pour cent) des incidents cybernétiques que le CST a désignés comme renfermant des communications privées. Le bureau a examiné : les rapports internes et externes; les cyberévénements qui ont été à l'origine des incidents, y compris le maliciel, les courriels, et les notes des analystes; ainsi que les détails contenus dans les outils et les bases de données, comme le nombre de communications privées, la justification de la conservation d'une communication privée particulière, et l'information sur l'auteur de la menace et sur le vecteur de la menace.

VECTEUR DE LA MENACE

On entend par « vecteur de la menace » la voie ou l'outil qu'utilise l'auteur de la menace pour attaquer une cible. À titre d'exemple, l'auteur d'une menace pourrait utiliser les vecteurs suivants pour attaquer une cible : un faux site Internet, des liens ou des pièces jointes dans un courriel ou des appareils mobiles.

Le commissaire a pu établir que les communications privées identifiées par le CST pendant la période visée par l'examen avaient été interceptées de manière non intentionnelle – le CST n'avait pas visé les Canadiens ou toute autre personne au Canada dans le cadre de ses activités de cyberdéfense. Les communications privées interceptées se rapportaient uniquement à la signature du maliciel et au comportement anormal du système. Les communications privées utilisées et conservées par le CST qui ont fait l'objet de l'examen étaient essentielles à la réalisation de la partie *b)* du mandat du CST, et les rapports se fondant sur les communications privées renfermaient des renseignements essentiels pour pouvoir identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada. Le CST a traité les communications privées interceptées conformément à ses politiques et à ses procédures. Le commissaire n'a constaté aucun cas où le CST aurait conservé une communication privée au-delà des périodes de conservation et de destruction prescrites par ses politiques.

En 2015-2016, il y a eu une augmentation importante du nombre de communications privées interceptées. Il est encourageant de voir que dans le rapport de fin d'exercice présenté au ministre sur les autorisations ministérielles de 2015–2016, le CST a continué de présenter la répartition du nombre de communications privées identifiées lors de la prestation de nouveaux services de cyberdéfense à plusieurs institutions du gouvernement du Canada. Au nombre des raisons expliquant l'augmentation par rapport à l'année dernière figurent la couverture élargie du réseau et l'accès à plus de données, les capacités de détection améliorées et l'automatisation de l'analyse.

Comme c'était le cas au cours des années passées, la majorité des communications privées que le CST a dénombrées comme étant conservées ou utilisées en 2015–2016 consistaient en des courriels non sollicités envoyés par l'auteur d'une cybermenace à un employé du gouvernement du Canada et ne renfermant rien de plus qu'un code malveillant ou un élément d'ingénierie sociale – c'est-à-dire qu'il n'y avait pas d'échange d'information personnelle ou d'autre information significative entre l'auteur de la cybermenace et l'employé. Le CST fait preuve de prudence et dénombre toutes ces communications comme étant des communications privées. En conséquence de la méthode de dénombrement du CST, il semble que les activités de cyberdéfense donnent lieu à l'interception non intentionnelle d'un nombre beaucoup plus grand de communications privées que les activités du CST liées à la collecte de renseignements électromagnétiques étrangers. En 2015, le commissaire avait recommandé que les rapports du CST présentés au ministre mettent en lumière les différences importantes entre les courriels à destination ou en provenance du Canada interceptés dans le cadre des activités de cyberdéfense et les communications privées interceptées dans le cadre des activités de collecte de renseignements électromagnétiques étrangers, y compris les attentes moins élevées à l'égard de la protection de la vie privée rattachées aux communications privées interceptées dans le cadre des activités

de cyberdéfense. Au moment où a été réalisé l'examen, le CST a fait observer qu'il se penchait sur la question de savoir si cette interprétation juridique des communications privées s'applique aux activités de cyberdéfense. Il n'en demeure pas moins qu'aux yeux du commissaire, une communication ne renfermant rien de plus qu'un code malveillant ou un élément d'ingénierie sociale envoyé à un système informatique de façon à lui porter atteinte n'est pas une communication privée au sens du *Code criminel*.

Il est encourageant que le CST prenne aussi des mesures pour donner suite aux autres constatations et pour mettre en œuvre les recommandations formulées au terme du dernier examen des activités de cyberdéfense, y compris :

- la diffusion de nouvelles lignes directrices et de communications régulières à l'intention de la direction et des employés opérationnels sur les changements touchant la politique;
- le renforcement de l'exactitude et de la cohérence dans les rapports au ministre;
- la mise en place d'un nouveau cours obligatoire sur la politique pour aider les analystes à mieux comprendre ses exigences;
- l'amélioration de la tenue des dossiers grâce au déploiement prévu d'une nouvelle base de données pour la cyberdéfense; et
- l'adoption d'un marquage des communications privées plus détaillé et plus précis – notamment des explications plus complètes sur les raisons de la conservation d'une communication privée – ce qui a fourni au commissaire des preuves plus solides de la conformité et a facilité la conduite de l'examen.

CONCLUSION

Le CST n'a pas apporté de changements importants à la façon dont il mène ses activités de cyberdéfense ni aucun changement qui aurait présenté un risque pour la conformité à la loi ou la protection de la vie privée. Le commissaire a pu établir que les communications privées identifiées par le CST pendant la période visée par l'examen avaient été interceptées de façon non intentionnelle, c'est-à-dire que les activités de cyberdéfense du CST ne visaient ni des Canadiens ni des personnes se trouvant au Canada.

Les communications privées conservées ou utilisées ayant fait l'objet de l'examen étaient essentielles pour permettre au CST de s'acquitter de la partie ***b)*** de son mandat, et les rapports fondés sur les communications privées renfermaient de l'information essentielle pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

Le bureau du commissaire surveillera les mesures que prendra le CST pour régler les problèmes mis en évidence dans l'examen et il continuera de mener des examens annuels des activités de cyberdéfense exercées sous le régime d'une autorisation ministérielle.

7. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électroniques étrangers et des vérifications ponctuelles des « communications canadiennes » (2015-2016 et 2016-2017)

CONTEXTE

Le présent résumé combine les constatations découlant de l'examen annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électroniques étrangers et deux vérifications ponctuelles de « communications canadiennes ». L'examen des autorisations ministérielles relatives à la collecte des renseignements électromagnétiques étrangers a été réalisé en vertu de la ***Loi sur la défense nationale***, qui exige que le commissaire procède à l'examen des activités du CST exercées sous le régime d'autorisations ministérielles pour en contrôler la conformité et qu'il adresse au ministre un rapport annuel sur l'examen. Le bureau a également examiné le statut, à la fin de la période de validité des autorisations ministérielles, des communications privées conservées ou utilisées par le CST qui avaient été interceptées sous le régime de ces autorisations ministérielles. Les vérifications ponctuelles portaient sur des « communications canadiennes » conservées, utilisées ou détruites par le CST pendant les périodes précisées.

CANADIEN

On entend par **Canadien** un citoyen canadien, un résident permanent au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés* ou une personne morale constituée ou prorogée sous le régime d'une loi fédérale ou provinciale.

COMMUNICATION PRIVÉE ET « COMMUNICATION CANADIENNE »

La **communication privée** est ainsi définie à l'article 183 du *Code criminel* : « communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine. »

Une « **communication canadienne** » désigne une communication entre deux interlocuteurs dont l'un se trouve physiquement au Canada (c'est-à-dire une communication privée) ou est un Canadien qui se trouve physiquement à l'extérieur du Canada. Une telle communication peut être acquise soit par le CST, soit par les partenaires de la Collectivité des cinq et transmise au CST.

Le CST mène des activités de collecte de renseignements électromagnétiques étrangers en vertu de l'alinéa 273.64(1)*a)* de la *Loi sur la défense nationale* – partie *a)* du mandat du CST – soit acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement. Ces activités ne peuvent viser des Canadiens ou toute personne au Canada, et elles doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés [alinéas 273.64(2)*a)* et *b)* de la *Loi sur la défense nationale*].

En vertu du paragraphe 273.65(1) de la *Loi sur la défense nationale*, le ministre peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le CST à intercepter des communications privées liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Comme les activités de collecte de renseignements électromagnétiques étrangers comportent un risque d'interception non intentionnelle de communications privées, le CST doit exercer ces activités sous le régime d'une autorisation ministérielle. Une communication privée interceptée peut être conservée ou utilisée par le CST uniquement si elle est jugée essentielle aux affaires internationales, à la défense ou à la sécurité. Tous les renseignements recueillis qui sont utilisés dans un rapport sur les renseignements étrangers sont conservés pendant une période indéterminée par le CST.

AUTORISATIONS MINISTÉRIELLES

Les autorisations ministérielles permettent au CST de passer outre l'interdiction d'intercepter des communications privées énoncée à la partie VI du *Code criminel*. Il s'agit d'un document écrit en vertu duquel le ministre de la Défense nationale autorise le CST à entreprendre une activité ou une catégorie d'activités comportant un risque d'interception non intentionnelle de communications privées. Les autorisations ne peuvent demeurer en vigueur pendant une période de plus d'un an. Pour en apprendre davantage sur les autorisations et les limites imposées aux activités du CST, veuillez consulter le site Web du bureau.

INTERCEPTION FORTUITE OU NON INTENTIONNELLE?

Pour décrire l'interception d'une communication privée sous le régime d'une autorisation ministérielle, le CST emploie le mot « fortuit » (*incidental*) tandis que le bureau du commissaire emploie le terme « non intentionnel ». Pourquoi et quelle est la différence entre les deux qualificatifs?

Il y a interception « fortuite » d'une communication privée lorsque le CST intercepte une communication entre une entité étrangère située à l'extérieur du Canada et une personne au Canada.

Le terme « non intentionnel » constitue une description légale de l'interception « fortuite » d'une communication privée par le CST dans un contexte technique ou opérationnel. Ainsi, du point de vue légal, on peut dire de l'interception qu'elle était « non intentionnelle » puisqu'elle ne visait pas un Canadien ou une personne au Canada. Il s'agit plutôt d'un sous-produit ou d'un élément accessoire découlant du ciblage d'une entité étrangère située à l'extérieur du Canada.

Au cours de l'exercice 2016–2017, le CST a mené des activités de collecte de renseignements électromagnétiques étrangers sous le régime d'autorisations ministérielles, dont trois étaient en vigueur du 1er juillet 2015 au 30 juin 2016 et les trois autres du 1er juillet 2016 au 30 juin 2017. Le bureau s'est penché sur ces autorisations ministérielles.

Les objectifs de l'examen étaient les suivants : veiller à ce que les activités aient été autorisées par le ministre, c'est-à-dire que les conditions d'autorisation énoncées au paragraphe 273.65(2) de la ***Loi sur la défense nationale*** ont été remplies; relever tout changement important – survenu dans l'année ou les années visées par l'examen comparativement aux années antérieures – aux documents d'autorisation ministérielle eux-mêmes ainsi qu'aux activités du

CST ou à une catégorie d'activités décrites dans les autorisations ministérielles; et évaluer les répercussions des changements, le cas échéant, sur le risque de non-conformité à la loi ou le risque pour la vie privée.

Le bureau a examiné le statut, à la fin de la période de validité des autorisations ministérielles de 2015–2016, des communications privées identifiées que le CST avait acquises, conservées ou utilisées en exerçant ses activités de collecte de renseignements électromagnétiques étrangers. Le bureau a vérifié la conformité du CST à la loi et à toutes les autorisations, instructions ministérielles et politiques applicables, et a évalué la mesure dans laquelle le CST avait protégé la vie privée des Canadiens. En outre, le bureau du commissaire a fait deux vérifications ponctuelles, sans avoir donné de préavis au CST, de « communications canadiennes » (y compris des communications privées) utilisées ou conservées par le CST au cours des périodes allant du 1er mars 2016 au 31 mai 2016 et du 1er décembre 2016 au 15 janvier 2017.

Le bureau a examiné tous les rapports sur les renseignements étrangers établis par le CST qui se fondaient en totalité ou en partie sur des « communications canadiennes ». Le bureau a également reçu des comptes rendus sur l'ensemble des « communications canadiennes » conservées, il a vu de ses propres yeux un échantillon de ces communications et il a interviewé les analystes du renseignement étranger et les superviseurs concernés qui mettaient en œuvre les priorités du gouvernement en matière de renseignement au sujet des motifs sur lesquels ils s'appuyaient pour conserver les communications.

CONSTATATIONS ET RECOMMANDATIONS

Le commissaire a constaté que les autorisations ministérielles de 2015–2016 et de 2016–2017 relatives à la collecte de renseignements électromagnétiques étrangers remplissaient les conditions d'autorisation définies dans la ***Loi sur la défense nationale***, à savoir :

- l'interception vise des entités étrangères situées à l'extérieur du Canada;
- les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;
- la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée; et
- il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

Le commissaire n'a pas observé de changements importants dans les autorisations ministérielles de 2015–2016 et de 2016–2017 ni dans les mémoires de demande connexes adressés au ministre.

PROTECTION DE LA VIE PRIVÉE DES CANADIENS

Le CST se voit interdire, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, de cibler des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. Le fait que le travail du CST vise des cibles étrangères signifie que, à la différence des autres organismes de renseignement et de sécurité du Canada, le CST a des interactions limitées avec les Canadiens. Lorsque le CST acquiert fortuitement de l'information se rapportant à un Canadien, il est tenu par la loi de prendre des mesures pour protéger la vie privée de ce Canadien. Dans le cadre de son examen des activités du CST, le commissaire vérifie entre autres si le CST ne cible pas des Canadiens et s'il applique efficacement des mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités opérationnelles qu'il entreprend.

Une fois de plus cette année, en 2015–2016, il y a eu une hausse considérable du nombre de communications privées utilisées ou conservées (soit 3 348 communications privées, ce qui représente une hausse de près de 3 000 communications par rapport à 2014-2015) à la fin de la période de validité de l'autorisation ministérielle de 2015-2016. La hausse du nombre de communications privées utilisées ou conservées demeure une conséquence des caractéristiques techniques de technologies de communication particulières et de la manière dont le CST dénombre les communications privées.

De ces 3 348 communications privées, le CST a utilisé 533 communications privées dans 20 rapports sur les renseignements étrangers, et a par la suite détruit les communications privées restantes. Pendant les deux vérifications ponctuelles, le bureau a également examiné 40 pour cent des « communications canadiennes » qui avaient été non intentionnellement acquises par le CST lors des périodes visées par les vérifications, et identifiées comme telles par la suite. Ceci incluait tant des communications marquées pour conservation que des communications marquées pour destruction par le CST comme étant non essentielles aux affaires internationales, à la défense ou à la sécurité. Le bureau a confirmé que les « communications canadiennes » non essentielles ont été détruites.

Le commissaire a donc pu établir que la manière actuelle dont le CST dénombre les communications privées donne une vision déformée du nombre de Canadiens ou de personnes se trouvant au Canada qui sont interlocuteurs dans une communication interceptée par le CST pour obtenir des renseignements étrangers sous le régime d'autorisations ministérielles. Le commissaire a par conséquent **recommandé** que les rapports du CST adressés au ministre sur les communications privées renferment de l'information supplémentaire pour décrire plus précisément les communications privées et pour expliquer l'ampleur de l'atteinte à la vie privée.

À la lumière de l'information examinée et des entretiens menés, le commissaire a conclu que le CST avait agi en conformité avec la loi et qu'il avait protégé la vie privée des Canadiens. En particulier :

- les activités relatives à la collecte de renseignements électromagnétiques étrangers du CST ne visaient pas des Canadiens ou des personnes se trouvant au Canada;
- les « communications canadiennes » identifiées par le CST avaient été interceptées de façon non intentionnelle;
- les « communications canadiennes » utilisées et conservées par le CST étaient essentielles aux affaires internationales, à la défense ou à la sécurité, comme l'exige la *Loi sur la défense nationale*;
- le CST avait détruit les « communications canadiennes » non essentielles; et
- le CST avait exercé ses activités relatives à la collecte des renseignements électromagnétiques étrangers conformément aux directives et aux autorisations ministérielles et avait traité les « communications canadiennes » conformément à ses politiques et à ses procédures – le CST n'avait pas conservé de communications privées au-delà des périodes de conservation et de destruction prescrites par ses politiques.

COMMUNICATIONS ENTRE UN CONSEILLER JURIDIQUE ET SON CLIENT

Au cours de la période de validité de l'autorisation ministérielle de 2015-2016, le CST a signalé au ministre qu'il avait utilisé, pour la première fois, une communication privée considérée comme étant une communication entre un client et son conseiller juridique.

Le privilège du secret professionnel de l'avocat renvoie au droit quasi constitutionnel de communiquer de façon confidentielle avec son conseiller juridique, un droit qui est particulièrement protégé par les tribunaux. Le CST s'est doté d'une politique et de mesures pour déterminer si ce type de communication peut être utilisé dans un rapport. Au moment où la communication a été obtenue,

la politique du CST exigeait qu'un avis juridique soit demandé au ministère de la Justice pour déterminer si la conservation ou l'utilisation d'une communication entre un conseiller juridique et son client était conforme aux lois canadiennes. L'exigence relative à la consultation du ministère de la Justice dans ces circonstances ne fait désormais plus partie de la politique du CST.

L'examen de cette communication particulière a été toutefois entravé par l'absence de documentation sur l'avis juridique obtenu ou de possibilité d'interroger l'avocat au dossier. Par conséquent, le bureau a dû se fier aux déclarations des fonctionnaires du CST. Après examen, le bureau a convenu que la communication ne constituait pas en fait une communication entre un conseiller juridique et son client. Le CST n'aurait donc pas été tenu de signaler cette activité au ministre. Nonobstant ce qui précède, et bien que le commissaire n'ait pas eu d'autres questions sur le traitement de la communication par le CST, le commissaire estimait que le CST aurait dû obtenir un avis juridique écrit auprès du ministère de la Justice concernant le caractère privilégié de la communication et concernant la question de savoir si son utilisation ou sa conservation était conforme aux lois canadiennes et si elle n'allait pas déconsidérer l'administration de la justice.

En raison de la nature quasi constitutionnelle de la protection accordée aux communications entre un conseiller juridique et son client, le commissaire **a recommandé** que le CST obtienne toujours un avis juridique écrit auprès du ministère de la Justice concernant la conservation ou l'utilisation d'une communication interceptée qui est protégée par le secret professionnel de l'avocat.

CONCLUSION

Il est encourageant de constater qu'au cours des dernières années, le CST a mis en œuvre les recommandations du commissaire conseillant d'élargir la portée des rapports présentés au ministre sur la protection de la vie privée. Les rapports sur la protection de la vie privée incluent maintenant les « communications canadiennes » identifiées par le CST et reçues par l'intermédiaire d'un allié et celles auxquelles participe un Canadien se trouvant à l'étranger, deux types de communications qui sont réputés présenter un intérêt similaire à celui présenté par les communications privées du point de vue de la protection de la vie privée. Pour donner suite à une autre recommandation du commissaire, les rapports sur la protection de la vie privée présentés par le CST au ministre renferment désormais des renseignements plus détaillés sur les communications privées conservées tirées de renseignements électromagnétiques étrangers, y compris le nombre mensuel de communications privées conservées et les justifications de la conservation.

Le bureau du commissaire continuera d'effectuer des examens annuels des autorisations ministérielles liées à la collecte des renseignements électromagnétiques étrangers ainsi que des examens des activités de collecte de renseignements électromagnétiques étrangers exercées par le CST sous le régime des autorisations ministérielles. Le bureau procédera également à des vérifications ponctuelles approfondies des « communications canadiennes » acquises et identifiées par le CST, qu'elles aient été recueillies par le CST ou par un allié. En outre, dans le cadre d'un examen de suivi, le commissaire se penchera sur les nouvelles activités relatives à la collecte des renseignements électromagnétiques étrangers exigeant la coopération du CST avec les Forces armées canadiennes. Enfin, le bureau du commissaire surveillera les mesures prises par le CST pour régler les questions relevées dans le présent rapport, y compris celle de l'utilisation et de la conservation des communications entre un conseiller juridique et son client.

PLAINTES CONCERNANT LES ACTIVITÉS DU CST

En 2016–2017, le bureau a été contacté par plusieurs personnes en quête d'information ou exprimant des préoccupations concernant les activités du CST. Toutefois, il a été déterminé que les demandes de renseignements ne relevaient pas du mandat du commissaire, ne se rapportaient pas aux activités opérationnelles du CST ou manquaient de sérieux. Aucune plainte concernant les activités du CST ne justifiait une enquête.

MANDAT SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

Le commissaire est tenu en vertu de la ***Loi sur la protection de l'information*** de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui ont l'intention de communiquer des renseignements opérationnels spéciaux – par exemple certains renseignements se rapportant aux activités du CST en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre n'a été signalée au commissaire en 2016–2017.

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Préserver la confiance des parlementaires et des Canadiens dans le travail du bureau exige ouverture et transparence, ainsi que des efforts concertés pour suivre le rythme des technologies en constante évolution et pour tirer parti des occasions d'échanger avec les homologues du bureau dans d'autres pays sur les pratiques exemplaires.

PARTICIPATION AU DIALOGUE SUR LA SÉCURITÉ NATIONALE ET LA REDDITION DE COMPTES

La sécurité nationale a été un sujet d'actualité au cours de la dernière année, avec les consultations publiques qui ont été tenues à l'échelle du pays et parrainées par le gouvernement. Le bureau a fourni des réponses à une série de questions préparées en vue des consultations sur la surveillance, y compris les organismes d'examen existants et le projet de comité de parlementaires sur la sécurité nationale. Le commissaire a écrit au ministre Goodale, qui supervise le processus de consultation, à propos d'une question précise pour lui faire part de son opposition à une proposition qui obligerait le CST à obtenir un mandat judiciaire, plutôt qu'une autorisation ministérielle, lorsque le CST intercepte une communication privée de façon non intentionnelle.

Ces consultations mises à part, le commissaire a comparu devant des comités parlementaires pour présenter son point de vue sur la législation qui touche aux questions liées à la reddition de comptes, au CST et au travail du bureau :

- **Comité permanent de la sécurité publique et nationale de la Chambre des communes, 15 novembre 2016** : Le commissaire a comparu devant ce comité relativement au projet de loi C-22, qui propose la mise sur pied d'un comité de la sécurité nationale et du renseignement composé de parlementaires. Encouragé par la reddition de comptes et la transparence accrues qu'un tel comité pourrait apporter aux activités relatives à la sécurité nationale et au renseignement, le commissaire a expliqué en quoi le comité agirait également comme catalyseur de la collaboration entre les organismes d'examen. Le commissaire a fait observer que le mandat général du comité et les rôles respectifs des organismes d'examen et du comité proposé devraient être clairement définis pour éviter le double emploi et assurer la complémentarité;
- **Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes, 7 décembre 2016** : Le commissaire a discuté de la première année de la mise en œuvre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* – qui a trait à la communication d'information entre les ministères et organismes responsables de la sécurité et du renseignement au Canada. Bien que le CST n'ait pas reçu ni communiqué d'information en vertu de la *Loi* au cours de la première année, le commissaire a repris à son compte les préoccupations du commissaire à la protection de la vie privée du Canada selon lesquelles le seuil au-delà duquel l'information est communiquée ne tient pas compte de la présence de renseignements personnels, et que le seuil au-delà duquel les renseignements personnels en particulier sont communiqués devrait être plus élevé;

- **Comité permanent de la défense nationale de la Chambre des communes, 21 mars 2017** : Le commissaire a décrit quatre enjeux importants, dont les changements devant être apportés à la *Loi sur la défense nationale*, les éclaircissements nécessaires au projet de loi C-22 sur la façon dont les organismes d'examen travailleront avec le comité de parlementaires proposé, la nécessité que la coopération entre les organismes d'examen soit autorisée par la loi, ainsi que l'importance de la transparence pour les organismes responsables de la sécurité et du renseignement et leurs organismes d'examen respectifs dans le renforcement de la reddition de comptes globale et de la confiance du public.

Les allocutions et les lettres du commissaire se trouvent sur le site Web du bureau.

SENSIBILISATION, APPRENTISSAGE ET RÉSEAUTAGE

Le processus d'examen du bureau s'appuie sur une compréhension profonde de la politique et des activités du CST. Dans ce contexte, la formation des employés du bureau chargés des examens inclut les mêmes cours offerts par le CST à ses employés. Pour sa part, le bureau a continué de faire des présentations sur le rôle et le travail du commissaire dans le cadre des séances d'orientation à l'intention des nouveaux employés du CST.

Les employés du bureau se tiennent au courant des questions liées au renseignement et à la sécurité, à la protection de la vie privée, aux technologies et aux aspects légaux en participant à une variété de cours offerts par les institutions gouvernementales, les associations professionnelles et les universités. Au nombre des conférences auxquelles ont assisté les employés l'année dernière figurent la Conférence internationale sur le risque cybernétique et la Conférence sur l'éducation à la sécurité à Toronto. À la 18e conférence annuelle sur la sécurité et la protection de la vie privée qui s'est tenue à Victoria, en Colombie-Britannique, le directeur exécutif a agi comme animateur et présentateur au sein d'un groupe travaillant à la question « Vie privée, sécurité nationale et reddition de comptes : comment préserver la confiance du public? ». Faisaient également partie du groupe des représentants des médias, du Commissariat à la protection de la vie privée et du CST ainsi qu'un ancien avocat général de la National Security Agency des États-Unis.

La participation à des colloques sur les affaires internationales, la sécurité des technologies de l'information, la sécurité nationale, la protection de la vie privée et la cybersécurité ont été d'autres occasions d'apprentissage, de sensibilisation et de réseautage. Au nombre des organisations hôtes figuraient l'Association internationale des professionnels de la protection de la vie privée, le Réseau intégré sur la cybersécurité, le groupe de la direction du Programme canadien de coopération de la Défense et l'Association canadienne pour les études de renseignement et de sécurité. En janvier 2017, l'avocat interne du bureau s'est

adressé aux étudiants en droit de l'Université d'Ottawa pour leur expliquer le mandat et le rôle du bureau. Le bureau a aussi continué d'apporter son soutien au Canadian Network for Research on Terrorism, Security and Society (TSAS), mis sur pied par plusieurs universitaires.

ORGANISMES D'EXAMEN CANADIENS ET ÉTRANGERS

Le commissaire et le président du Comité de surveillance des activités de renseignement de sécurité (CSARS), ainsi que leurs hauts fonctionnaires ont poursuivi les discussions sur la coopération nationale et internationale. Ceux-ci et la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) ont aussi comparu ensemble devant les comités parlementaires chargés d'examiner le projet de loi C-22 et la *Loi sur la communication d'information ayant trait à la sécurité du Canada*.

Des discussions fructueuses avec les homologues à l'étranger ont marqué l'automne 2016. Le commissaire et les hauts fonctionnaires ont rencontré des membres du Intelligence and Security Committee of Parliament du Royaume-Uni. Les questions liées à la transparence et à la confiance du public ainsi que les relations entre un organisme d'examen parlementaire comme celui du Royaune-Uni et les organismes d'examen existants ont fait l'objet de discussions. Le président du comité du Royaume-Uni a fait observer que les organismes de surveillance et d'examen des deux pays font face à des défis similaires, en particulier pour ce qui est de surveiller l'équilibre entre la protection de la vie privée et la sécurité.

Toujours à l'automne, le commissaire et les hauts fonctionnaires du bureau ont rencontré David Anderson, l'examinateur indépendant des lois antiterrorisme au Royaume-Uni. Parmi les nombreux sujets abordés figurait l'évaluation de M. Anderson de la mise à jour de 2016 du projet de loi sur les pouvoirs d'enquête du gouvernement britannique, dans laquelle M. Anderson indiquait que le projet de loi [traduction] « introduit les normes les plus rigoureuses en matière de transparence » et qu'il « autorise légalement un éventail de pouvoirs dont la valeur a été démontrée. » Le projet de loi a été adopté en novembre.

Enfin, le commissaire, le directeur exécutif et leurs collègues du CSARS ont discuté de questions d'intérêt commun avec les organismes de surveillance et d'examen de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis au cours d'une réunion à Washington, D.C. De telles réunions deviendront plus importantes non seulement pour en apprendre davantage sur les pratiques exemplaires en matière d'examen et de surveillance, mais aussi pour savoir comment les organismes d'examen de la Collectivité des cinq peuvent se pencher plus efficacement sur les relations entre leurs organismes du renseignement afin d'accroître la confiance du public dans leurs pays respectifs.

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Le commissaire adopte une approche préventive axée sur le risque pour réaliser ses examens, établissant les priorités en matière d'examen en se concentrant sur les domaines où les risques de non-conformité à la loi et d'atteinte à la vie privée des Canadiens sont évalués comme étant les plus élevés. Un plan de travail triennal est mis à jour deux fois par an. L'élaboration du plan de travail repose sur maintes sources, notamment les séances d'information régulières du CST sur les nouvelles activités et les changements touchant les activités existantes, le rapport annuel classifié présenté par le chef du CST au ministre et faisant état des priorités du CST et des questions importantes sur le plan juridique, politique, opérationnel ou en matière de gestion, et les problèmes relevés dans les examens passés ou en cours. Pour apprendre davantage sur l'approche préventive axée sur le risque adoptée par le commissaire pour effectuer ses examens, veuillez consulter le site Web du bureau.

Quatre examens amorcés en 2016–2017 seront achevés en 2017–2018 : un examen portant sur une méthode particulière de collecte de renseignements électromagnétiques étrangers menée sous le régime d'une autorisation ministérielle et d'une directive ministérielle; un examen axé sur les activités de ciblage du CST; un examen distinct amorcé en 2016-2017 qui fait suite à l'examen achevé sur le partage de renseignements par le CST avec des entités étrangères; un examen annuel des divulgations d'information sur l'identité de Canadiens à des clients du gouvernement du Canada, à des alliés et à des entités n'appartenant pas à la Collectivité des cinq.

Un examen de suivi sera mené, qui portera sur l'aide fournie par le CST au Service canadien du renseignement de sécurité (SCRS) en vertu de la partie *c)* de son mandat et des articles 12 et 21 de la ***Loi sur le Service canadien du renseignement de sécurité*** (appelés à l'origine « Mandats d'interception au Canada de télécommunications étrangères »). Cet examen était censé commencer l'an passé, mais il a été déplacé dans l'ordre des priorités étant donné l'examen non prévu mentionné plus haut. Un autre examen de suivi sera également mené qui portera sur le soutien apporté par le CST au SCRS en vertu de la partie *c)* de son mandat concernant un certain type de rapport mettant en cause des Canadiens. Une étude sur l'utilisation des plateformes Internet internes par le CST à des fins de partage de renseignements sera également réalisée cette année.

En outre, le commissaire continuera d'effectuer des examens annuels portant sur :

- les autorisations ministérielles de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, y compris les vérifications ponctuelles de « communications canadiennes » acquises et identifiées par le CST;
- les divulgations par le CST d'information sur l'identité de Canadiens; et
- les incidents liés à la vie privée et les erreurs de procédure mises au jour par le CST ainsi que les mesures qu'il a prises par la suite pour y remédier.

ANNEXE A : BIOGRAPHIE DE L'HONORABLE JEAN-PIERRE PLOUFFE, CD

L'honorable Jean-Pierre Plouffe a été nommé commissaire du Centre de la sécurité des télécommunications le 18 octobre 2013 pour un mandat de trois ans. Le 18 octobre 2016, son mandat a été renouvelé pour une période de deux ans.

Né le 15 janvier 1943 à Ottawa, en Ontario, M. Plouffe a fait ses études à l'Université d'Ottawa où il a obtenu sa licence en droit ainsi qu'une maîtrise en droit public (droit constitutionnel et international). Il a été admis au barreau du Québec en 1967.

M. Plouffe a débuté sa carrière au cabinet du juge-avocat général des Forces armées canadiennes. Il a pris sa retraite de la Force régulière en 1976, alors qu'il était lieutenant-colonel, mais est demeuré dans la Force réserve jusqu'en 1996. Il a été avocat en pratique privée au sein du cabinet Séguin, Ouellette, Plouffe et associés, à Gatineau, au Québec, où il s'est spécialisé en droit criminel, a agi en tant que président du tribunal disciplinaire des pénitenciers fédéraux, ainsi qu'en tant qu'avocat de la défense en cour martiale. Par la suite, M. Plouffe a travaillé pour le bureau d'aide juridique en qualité de directeur de la section de droit criminel.

M. Plouffe a été nommé juge militaire en 1980 (Force de réserve), puis juge à la Cour du Québec en 1982. Pendant plusieurs années, il a été chargé de cours en procédure pénale à la Section de droit civil de l'Université d'Ottawa. Il a ensuite été nommé juge à la Cour supérieure du Québec en 1990 puis juge à la Cour d'appel de la cour martiale du Canada en mars 2013. Il a pris sa retraite en tant que juge surnuméraire le 2 avril 2014.

Au cours de sa carrière, M. Plouffe a participé à la fois à des activités professionnelles et communautaires. Il a reçu des distinctions honorifiques civiles et militaires.

ANNEXE B : EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* ET DE *LA LOI SUR LA PROTECTION DE L'INFORMATION* RELATIFS AU MANDAT DU COMMISSAIRE

Loi sur la défense nationale – Partie V.1

Nomination du commissaire et durée du mandat

273.63 (1) Le gouverneur en Conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge surnuméraire ou un juge à la retraite d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

Mandat

(2) Le commissaire a pour mandat :

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Rapport annuel

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

Loi sur les enquêtes

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

Assistance

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

[...]

Révision des autorisations

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Loi sur la protection de l'information

Défense d'intérêt public

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

[...]

Informer les autorités

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

a) la personne, avant la communication ou la confirmation, a informé de la question [...] l'administrateur général ou [...] le sous-procureur général du Canada;

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession, [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.